Abnormal SECURITY

Threat Research Report | Q1 2021

The Rising Threat of Vendor Email Compromise in a Post-SolarWinds Era

Executive Summary

SolarWinds-Style Email Attacks Going Mainstream

The historic attack on SolarWinds shook the cybersecurity industry in a profound way and opened the world's eyes to supply chain attacks. Nearly two months after public disclosure, we now know that it was a high-profile example of a vendor email compromise attack (VEC).

SolarWinds **stated** that an "email account was compromised and used to programmatically access accounts of targeted SolarWinds personnel in business and technical roles." The attack went undetected by its email security defenses for at least nine months, according to the *Wall Street Journal*. Numerous other vendors, including non-SolarWinds customers, have also disclosed attacks through the same technique.

These attacks are insidious because they bypass traditional email defenses that rely on threat intelligence to stop them. They exploit trusted communications between vendors and customers through personalization and social engineering. The impact is far-reaching and includes fraud and financial loss.

Abnormal Security sees clear evidence that the same technique used in the SolarWinds attack — vendor email compromise — is going mainstream. Its growth is accelerating and impacting many more industries than has been reported to date, including retail, manufacturing, energy and services. We're sharing this evidence through this research report to help CISO's understand its impact and how to defend their enterprises.

Between Q3 2020 and January 2021, the chance of companies getting hit with a vendor email compromise attack during any given week increased 82% with the maximum observed cost through various forms of fraud as much as $1.6M per attack.

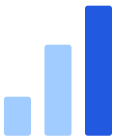
To counter these highly sophisticated attacks through trusted communications, large enterprise organizations need the right technical controls to identify vendors that have been compromised and also ensure they don't compromise their own customers. This is possible with a real-time risk assessment of vendors and customers communicating with your organization to stop supply chain fraud. With this, enterprises can protect themselves against the next SolarWinds vendor email compromise attack.

Sincerely,
Evan Reiser
CEO and Co-Founder, Abnormal Security

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Key Takeaways



Chance of Getting Hit with VEC Attack
during any given week

82%

increase from Q3 to January 2021

Maximum Observed Cost of a VEC Attack

$1.6M

Stopped by Abnormal Security

Average Cost of Vendor Email Compromise Attacks

$183K

observed and stopped by Abnormal Security

Average Cost of a Billing Account Update Fraud Attack

$300K

the costliest form of a VEC attack observed by Abnormal Security

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Q1 2021 State of Vendor Email Compromise

Chance of Getting Hit with VEC Attack
during any given week

82%
increase from Q3 to January 2021

The Probability of Vendor Email Compromise Increased

Vendor email compromise (VEC) occurs when an attacker has control of a vendor's email account. Vendor fraud occurs when attacks are sent from the compromised vendor account and/or an impersonated account with the goal of stealing money. These attacks often originate from "bad" IP addresses or include fraudulent "reply-to's" to direct the conversation away from the compromised account's inbox. In the case of attacks sent from an impersonated account, the attacker may or may not have access to the actual account.

Key Findings

- The **chance of companies getting hit with a VEC attack during any given week increased 82%** between Q3 2020 and January 2021 (Figure 1).
- **Companies had a 50% chance of getting hit with a VEC attack** at least once in Q4 vs. 40.2% in Q3 (see Figure 2).
- VEC cases in which the attacker poses as an existing vendor or customer were **sent from a compromised account 9.5%** of the time in Q4, up from 7.1% in Q3.

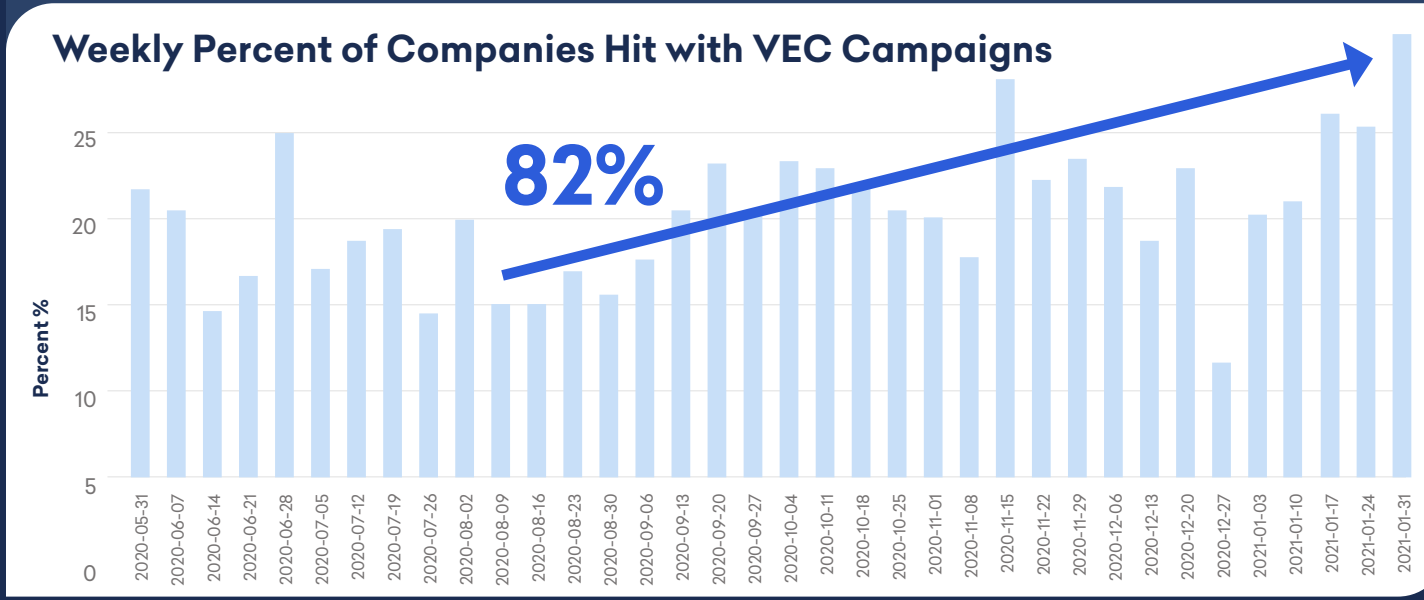


Figure 1. Chance of getting hit with a VEC attack January 2021 vs. Q3 2020

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

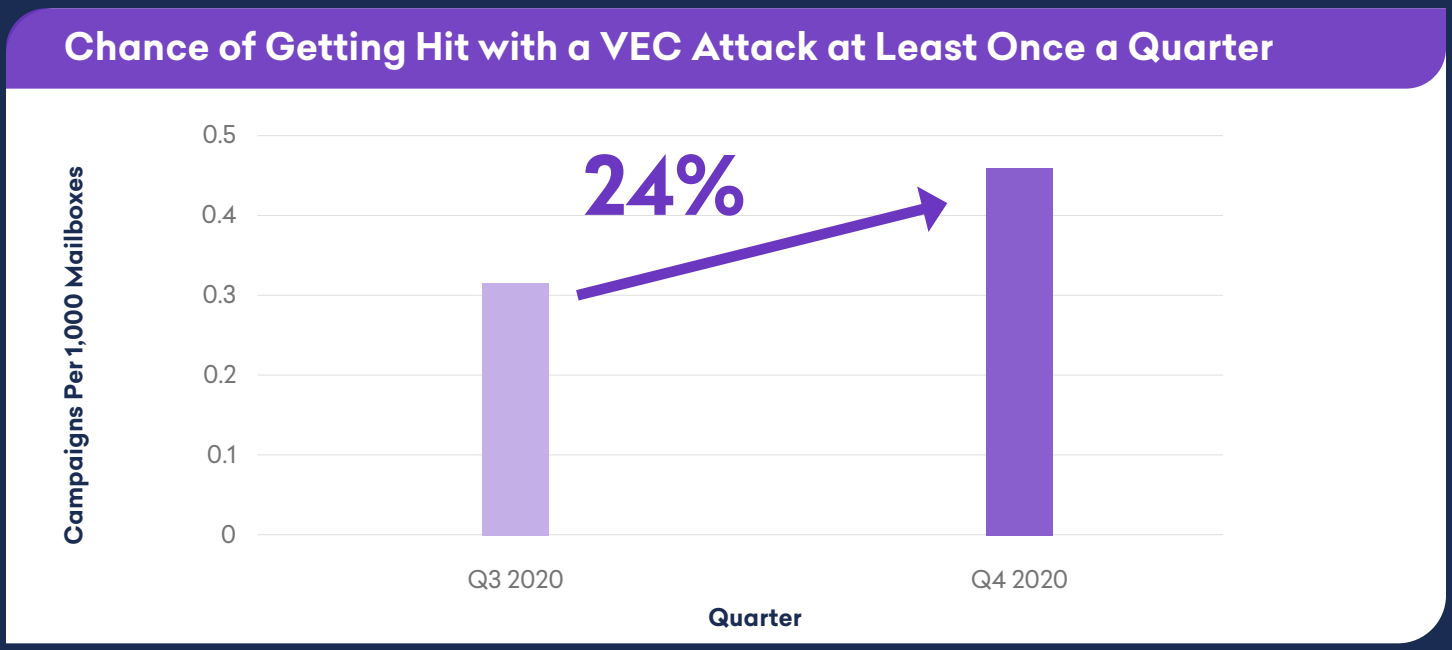


Figure 2. Chance of getting hit with a VEC attack, Q3-Q4 2020

Average Potential Cost of Vendor Email Compromise Exceeds Six Figures

The FBI's Internet Crime Complaint Center (IC3) actively tracks financial losses from BEC attacks. Its 2019 Internet Crime Report revealed that BEC crimes cost businesses $1.77B, with an average of $75,000 per complaint. This data, however, is based on complaints after attacks were successful. Abnormal Security is putting a spotlight on VEC-specific crimes by establishing an industry-first benchmark that tracks potential VEC-related costs.

We examined data for the sophisticated VEC attacks uniquely stopped by the Abnormal Security platform to determine their potential costs. For those campaigns where the dollar amount is known, the amounts exceed six figures on average and are 144% more costly than average BEC attacks.

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Maximum Observed Cost of a VEC Attack

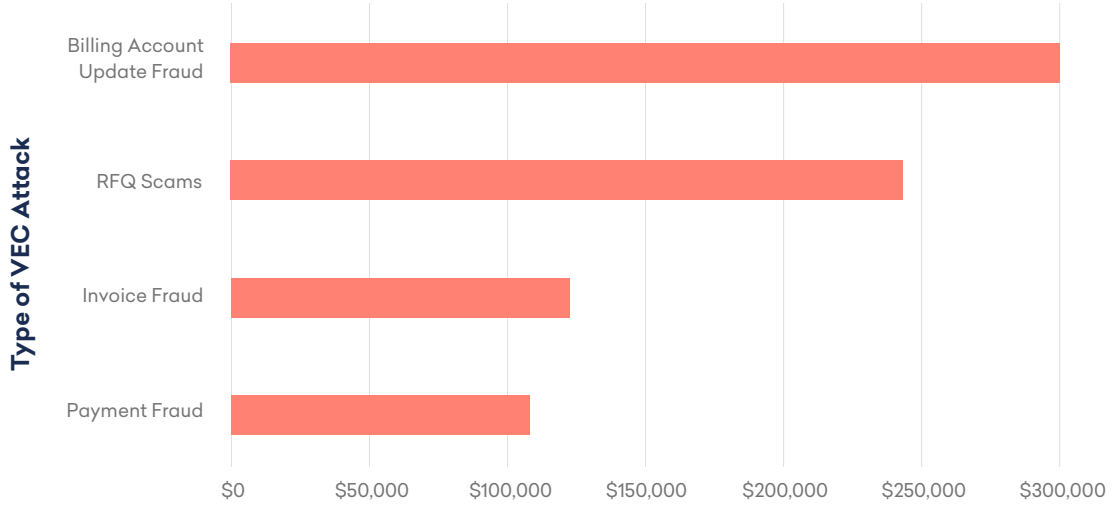
$1.6M

Stopped by Abnormal Security

Key Findings

- The **maximum observed cost** stopped by Abnormal Security is **$1.6 million**.
- The **average potential cost of vendor email compromise attacks is $183,000** depending on the goal of the attack.
- **Billing account update fraud is the costliest form of VEC attack — close to $300,000 on average per attack.**
- The **average potential cost of invoice fraud is $120,000**, with a **maximum of $466,000** identified and prevented.
- **Payment fraud attacks** fall on the lower end of the cost spectrum, **averaging $105,000 per attack with a maximum observed of $753,000**.
- Perhaps surprisingly, **RFQ scams**, which tend to be seen as less sophisticated than other VEC attack types, can be quite expensive. The **average seen by Abnormal Security in our dataset is $242,000 with a maximum of $500,000**.

Average Cost of VEC Attacks by Goal



© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Invoice and Payment Fraud BEC Attacks

44.5%

increase from Q3 to Q4 2020

Invoice/Payment Fraud Dominates Attack Landscape

Abnormal Security continues to see invoice/payment fraud as the most predominant form of BEC attack, with quarter-over-quarter growth continuing unabated.

Key Findings

- Threat actors continued to follow the money in Q4, as **weekly BEC campaigns with the goal of invoice/payment fraud increased 44.5%** from Q3 to Q4 (see figure 3).
- Invoice/payment fraud attacks **spiked in mid-December in the Retail/Consumer Goods & Manufacturing industry**.
- **COVID-19-related invoice/payment fraud attacks increased 107%** quarter-over-quarter in Q4 (see figure 4).

Weekly Invoice/Payment Fraud BEC Campaigns

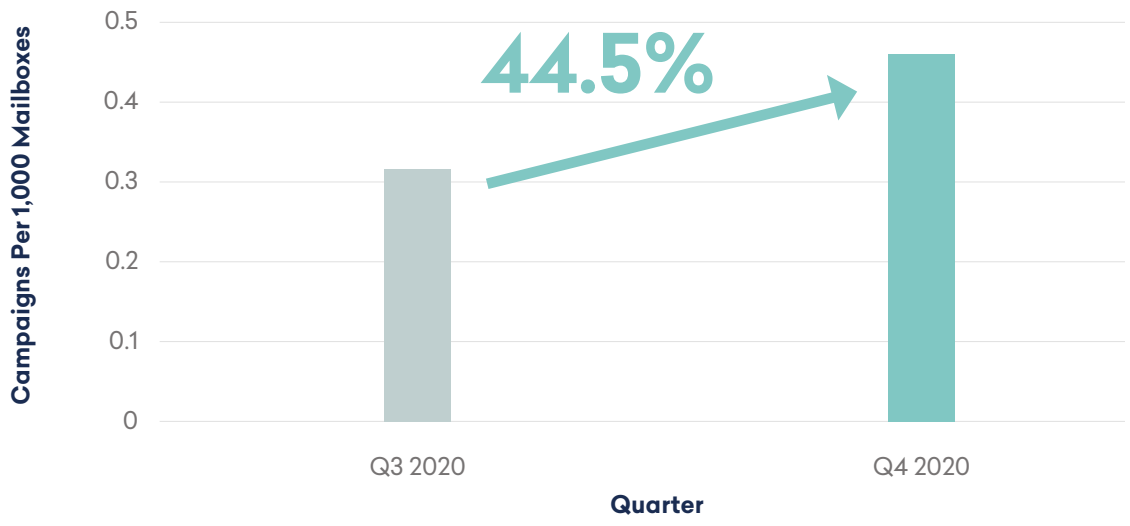


Figure 3. Median weekly invoice/payment fraud BEC campaigns in Q3 and Q4 (campaigns per 1,000 mailboxes)

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

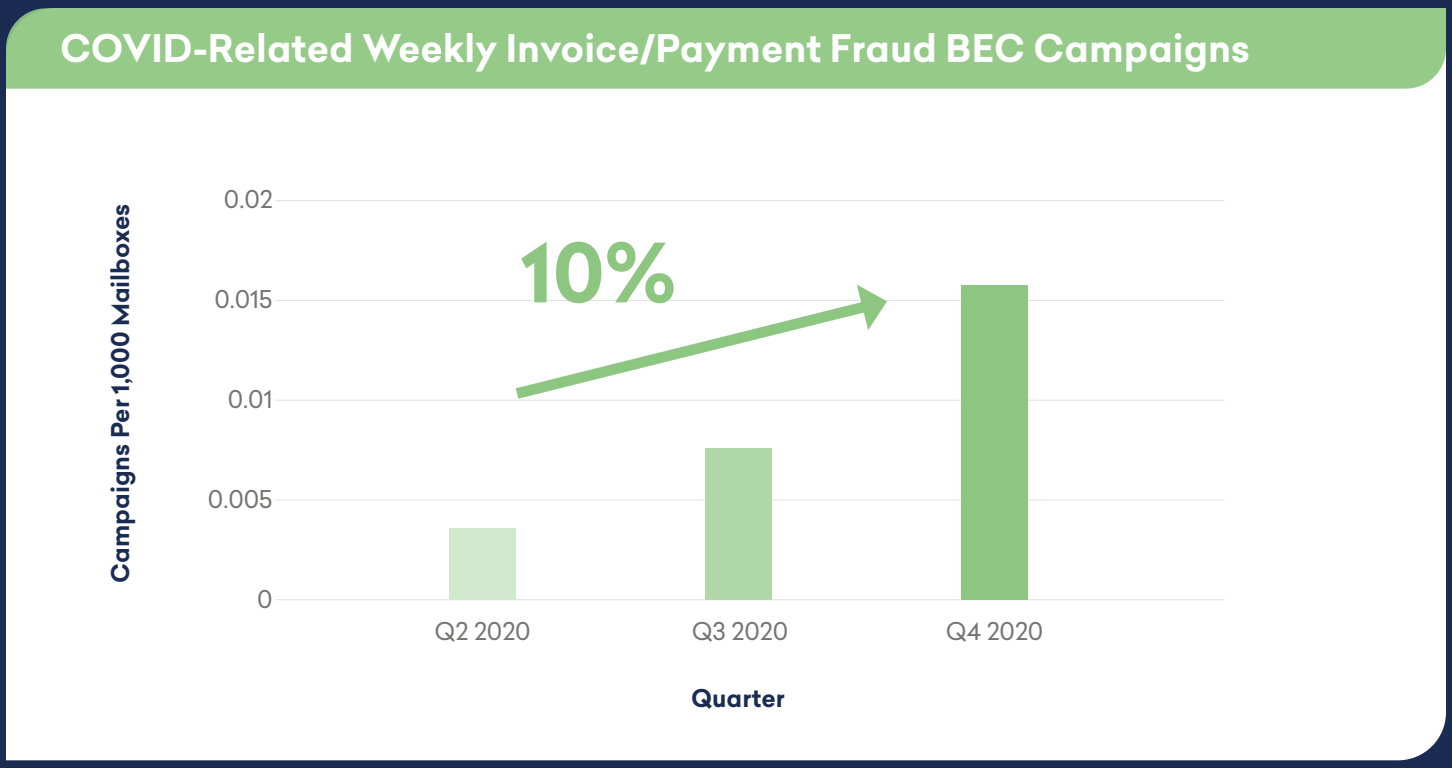


Figure 4. Median COVID-related weekly invoice/payment fraud BEC campaigns (campaigns per 1,000 mailboxes)

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

BEC Attacks Per Company

9.5%

increase from Q3 to Q4 2020

BEC Attack Volumes Rise Across Industries

As the only source of industry data on the true volume of BEC attacks, we continue to track an upward trajectory in the trendline overall and across almost all of the eight industries that we track, including Retail/ Consumer Goods & Manufacturing, Technology, Energy/Infrastructure, Services, Medical, Media/TV, Finance and Hospitality (see Appendix for more detail on industry subsegments).

BEC attacks historically are lower-volume and highly-targeted as compared to other types of email attacks, such as credential phishing. With a continued increase in volume every quarter, this low-volume truism is being challenged, which should elevate its priority as a security risk to address.

Further examining BEC attack trends across industries provides additional insight into where the volume increases are occurring. During Q4, we found that BEC attacks increased in seven out of eight industries.

Key Findings

- The **median number of BEC campaigns received per company each week increased 9.5%** from Q3 to Q4 (Figure 5).
- The **average rate of weekly BEC attacks more than doubled in 50% of industries** tracked by Abnormal Security.
- The average rate of weekly BEC attacks increased in Q4 in the following industries (see figure 6):

▲ 120%	▲ 112%	▲ 101%	▲ 100%	▲ 86%	▲ 73%	▲ 64%
Media/TV	Services	Hospitality	Energy/ Infrastructure	Technology	Retail/ Consumer Goods & Manufacturing	Finance

- The **average rate of weekly BEC attacks targeting the Medical industry decreased by 23%** from Q3 to Q4.

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

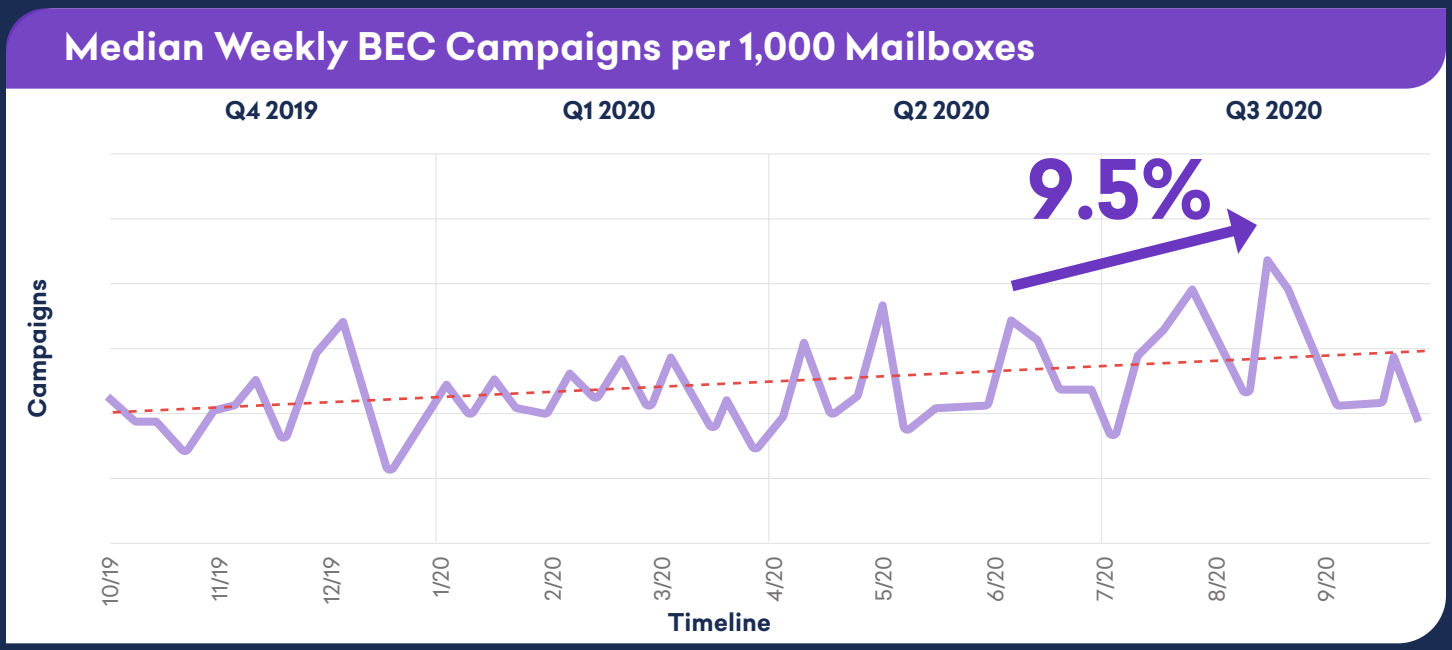


Figure 5: Median Weekly BEC Attacks Increased 9.5% from Q3 to Q4

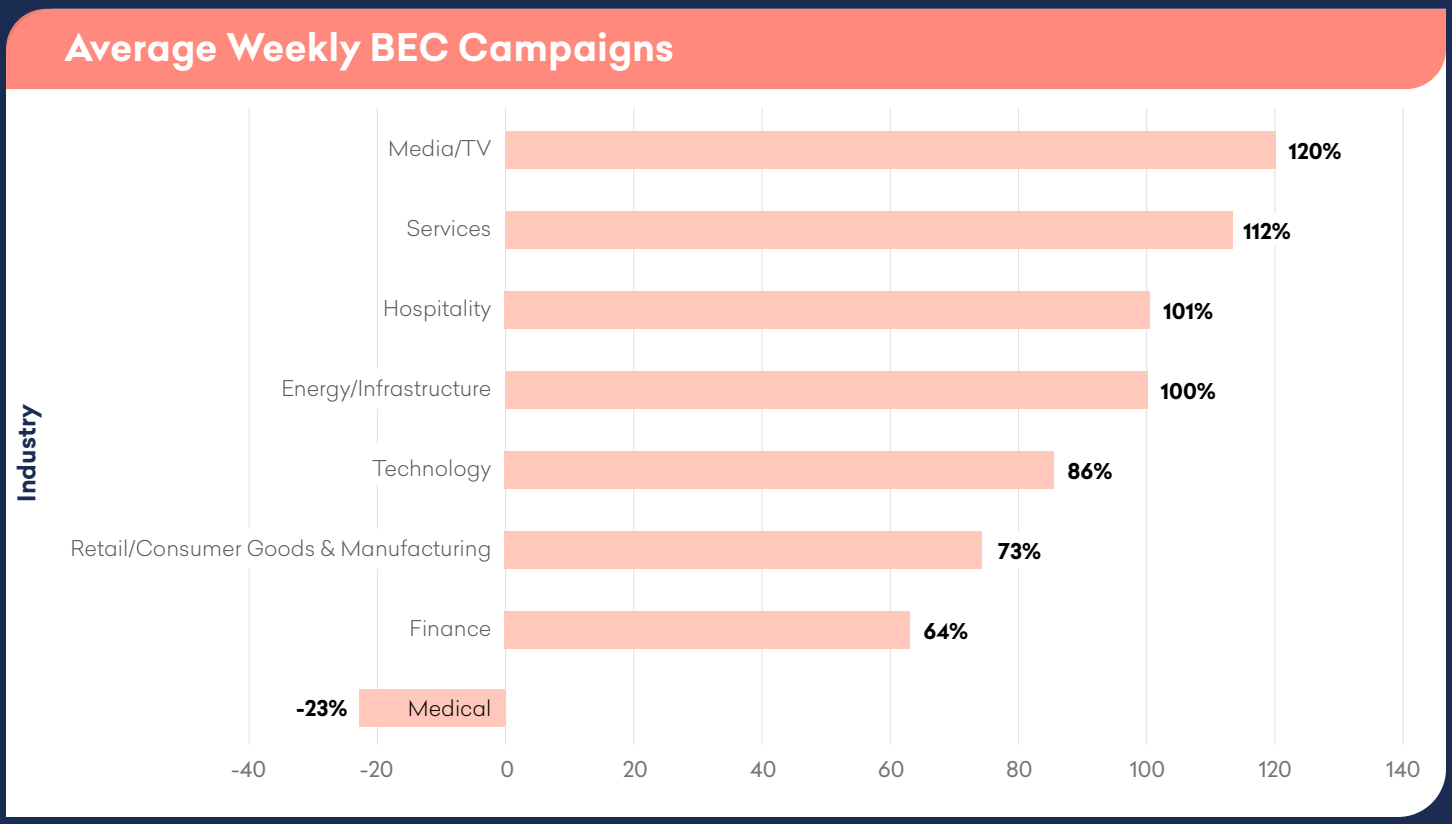


Figure 6: Percent Change in Average Weekly BEC Attacks Across Industries from Q3 to Q4

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Conclusion

Supply chain communications are trusted and typically convey a sense of urgency, making it easy for these types of attacks to blend in with legitimate and valid emails. Since the attacks come from trusted yet impersonated or compromised vendor accounts, organizations often cannot detect when an attack is underway until it's too late.

These attacks highlight the importance of tools to ensure supply chain security like VendorBase Abnormal's global, federated database of vendor and customer behaviors to stop supply chain compromise. VendorBase continuously monitors communications between vendors and partners, and provides a real-time, stateful risk assessment enabling Abnormal to stop these targeted supply chain attacks.

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Appendix

Industries included in each industry category considered in this analysis:

Industry Category	Sub-Industry
Retail/Consumer Goods & Manufacturing	Retail, Wholesale, Consumer Products, Manufacturing, Manufacturing — Durables, Manufacturing — Non-Durables
Technology	Technology, Computer Software, Social Media
Energy/Infrastructure	Energy / Utilities, Logistics / Transportation, Telecom / Communication Services
Services	Services, Professional Services, IT Services, Consulting
Medical	Medical Devices, Healthcare/Medical/Pharma, Hospitals / Health Care, Pharmaceuticals
Media/TV	Broadcast Media, Entertainment
Finance	Finance, Financial Services, Banking, Holding Companies, Venture Capital & Private Equity
Hospitality	Casinos & Gambling, Lodging, Restaurants

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY

Descriptions of Different Types of Fraud

Invoice Fraud

The target receives a fraudulent invoice with the attacker's bank details to trick the target into sending money to that bank. The legitimate-looking invoice with the fraudulent bank account details is usually attached to an email, but it is sometimes described within the body itself.

Billing Account Update Fraud

This is an attempt to update payment details of a recurring payment or an outstanding invoice. These attacks attempt to update payment details using similar phrases like "bank reconciliation audit" and needing to send money to a "secondary bank account."

Payment Fraud

Payment fraud is defined as any email that attempts to steal money and goods from a target through means that doesn't involve a specific invoice or payment transaction. These messages try to initiate contact with the customer or inquire about a payment transaction.

Payment fraud attacks can take different forms, including RFQ scams (an attempt to get customers to send goods to attackers without paying for it) and invoice inquiries (an attempt to initiate invoice fraud by asking customers to provide attackers with information about existing invoices).

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal SECURITY