Cybercriminals step up social engineering during pandemic

Cybercriminals have been going to great lengths throughout 2020 to get their hands on confidential information such as log-in details that let them bypass a company's security systems and commit theft or fraud by manipulating employees using fake or doctored emails. While this form of online social engineering had declined from Q4 2019 to Q1 2020, the arrival of the global pandemic provided cybercriminals with the perfect cover for ramping up email attacks. Coinciding with the increase in remote working during the second quarter, our global data has shown employees have been more likely to fall for social engineering scams, with organizations in the middle market most likely to be victimized.

Social engineering – Techniques such as email phishing used to manipulate someone into providing confidential information, e.g. log-in credentials, or taking other actions that bypass normal security to help the attacker commit theft or fraud.

Phishing – An email created to look like it comes from a trusted source that is designed to induce a recipient into sharing sensitive information, download malware or visit an infected website.

Fraudulent instruction – A social engineering attack in which compromised email credentials or spoofing are used to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by a cybercriminal.

Remote working poses challenge for prevention and detection

During the second quarter of 2020, cybercriminals had greater success in duping employees with phishing and social engineering scams. The number of incidents involving social engineering and business email compromise (BEC) reported to Beazley Breach Response (BBR) Services grew over Q1, even as the total incident count fell slightly.

The majority of social engineering attacks result in a BEC, where the cybercriminal gains access to an email account. However, in Q2 cybercriminals were most successful in stealing funds using social engineering techniques to provide fraudulent payment instructions without a system compromise.

With the expansion of the remote workforce, detecting and preventing social engineering scams has become more difficult. Employees are typically the first line of defense, but working remotely can make it harder for employees to maintain a culture of compliance. While the increase in distractions that come with caring for family members while working have been widely discussed, physical separation from the workplace is also a factor. Without a coworker to converse with at the next desk, employees are less likely to do a "sense check" of a suspicious email. In fact, BBR Services has handled an increase in notifications involving employees who admit they did not notice anything suspicious.

In another development, BBR Services has noted a slow-down in the speed at which companies detected that payments were being redirected, particularly if the change to payments had occurred near the beginning of the pandemic response.

Cybercriminals shift to the middle market; attacks become more sophisticated

Organizations in the middle market were increasingly likely to be targeted compared to smaller organizations, and reported 60% of these incidents, up from 46% in Q1. To the extent middle market organizations have been more resilient in carrying on day-to-day operations during the pandemic, their employees are more available to be targeted. And for cybercriminals, particularly those who can execute more sophisticated attacks, middle market organizations are richer targets.

Social engineering

incidents targeting middle market

46% Q1 2020 VS 60% Q2 2020

Attacker conceals diversion of vendor payments

One recent incident illustrates how attackers are becoming more sophisticated in avoiding detection, in this case through careful timing. The attacker gained access to the account of a university employee with responsibility for payments. Neither the email account nor remote access through the virtual private network (VPN) was protected by multi-factor authentication (MFA). The attacker determined which vendors were enrolled in the university's automated clearing house (ACH) system and the schedule on which they were paid. Over a six to eight week period, the attacker repeatedly went into the ACH system after hours, changed the banking information for those vendors, waited for payments to be processed, and then restored the original banking instructions before the start of the following day to avoid detection. Almost $600,000 of payments were diverted before the receiving bank identified the suspicious activity and shut it down.

Fraudulent instruction incidents grew in Q2

Not all scams require such sophistication to be successful. Social engineering incidents involving fraudulent instruction grew the most in Q2, compared to Q1, according to global figures reported by BBR Services. In these incidents, the victim's system is not always compromised, but the cybercriminals use social engineering to convince an employee to change wire instructions, thus diverting payments to an account they control, or to take some other action that leads to financial loss.

Fraudulent instruction

incidents targeting middle market

24% Q1 2020 VS 55% Q2 2020

Healthcare, financial institutions, manufacturing, real estate, and education were the most targeted industries in Q2 2020. Middle market organizations were again the primary target of all fraudulent instruction attacks, reporting 55% of incidents in Q2, compared to 24% in Q1 2020.

BBR Services – a dedicated team of experts

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage cyber incidents successfully. This in-house team of experts works closely with cyber policyholders on all aspects of incident investigation and breach response and coordinates the expert services that insureds need to satisfy legal requirements and maintain customer confidence.

In addition to managing data breach response, BBR Services provides a full range of resources to help mitigate risks before an incident occurs. BBR Services develops and maintains Beazley's risk management portal as well as coordinates newsletters and live expert webinars and pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops.

Prevention

Social engineering incidents that did involve a system infiltration remained at a steady rate in the first half of the year. In more than 80% of reported incidents, the attack is stopped before a direct financial loss, such as stolen funds, occurs. Cases in which cybercriminals manage to infiltrate a network generally require time-consuming forensic investigation to determine what data the cybercriminals have accessed and whether the compromise results in legal obligations to notify affected individuals.

Protecting your organization from social engineering and BEC doesn't need to be expensive. Modest investment in training and process changes can provide outsized returns, reducing the likelihood of falling victim.

- **Alert employees**, particularly those in accounting, finance, HR, and benefits, to be alert to these scams through security awareness campaigns. Provide periodic anti-fraud training that teaches all employees to detect and avoid phishing and social engineering scams.
- **Establish an out-of-band verification process** to confirm the identity of the person requesting a funds transfer, a change to banking information or payment instructions, or access to sensitive data such as tax and payroll information.
  - Require voice verification for all changes involving banking information.
  - **Don't trust** contact details provided in the request. If the request is fraudulent, the criminal will have supplied fake contact information, too.
  - If the request is by email, call and speak to the person at a number you know to be correct.
  - If the request is by phone, use an email address you know to be correct.
  - Instead of using "Reply," forward the email and type in the email address you know to be correct.
- **Set up MFA** for remote access to your email system, your VPN, your ACH system, and other sensitive applications. Many platforms now provide for MFA at little or no cost.
- **Tell customers** that you will not change banking instructions without authentication and to treat any such request as possibly fraudulent.
- **Reduce email retention periods** to limit the amount of data held in email inboxes.
- **Consider implementing email security improvements** such as the Sender Policy Framework (SPF) email security standard or an advanced email threat protection product.

beazley

www.beazley.com

BZCER044_US_09/20