Business email compromises (BEC), ransomware attacks and banking Trojans were key trends in 2018 and are continuing to evolve in 2019. These attacks do not discriminate in targeting businesses; all industry verticals and organizations of all sizes are falling victim to these crimes.

This Briefing provides an in-depth look at BEC, ransomware and banking Trojans using Beazley data as well as insight into how these crimes are perpetrated, the challenges posed and best practices for addressing them.

In 2018, Beazley Breach Response (BBR) Services managed over 3,300 data incidents reported by BBR insureds and the number of incidents managed by Beazley since 2009 crossed the 10,000 mark.

Data presented in this Breach Briefing is derived from incidents reported to Beazley in 2018.

\[\text{Accidental disclosure is still the top cause of loss for} \]
\[\text{Healthcare 31\%}\]

\[\text{AND}\]

\[\text{hack or malware increased by} \]
\[10 \text{ percentage points}\]

\[20\% \text{ to } 30\%\]

\[\text{Hack or malware incidents increased 10\% since last year due to the rise in business email compromise} \]

\[2017 37\% \text{ vs.} \quad 2018 47\%\]
Hack or malware is the top cause of loss in most industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial institutions</td>
<td>59%</td>
</tr>
<tr>
<td>Higher education</td>
<td>50%</td>
</tr>
<tr>
<td>Professional services</td>
<td>59%</td>
</tr>
<tr>
<td>Retail</td>
<td>62%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>56%</td>
</tr>
<tr>
<td>Real estate</td>
<td>57%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>67%</td>
</tr>
</tbody>
</table>

Top causes of loss in 2018

<table>
<thead>
<tr>
<th>Cause</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hack or malware</td>
<td>47%</td>
</tr>
<tr>
<td>Accidental disclosure</td>
<td>20%</td>
</tr>
<tr>
<td>Insider</td>
<td>9%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>8%</td>
</tr>
<tr>
<td>Portable device</td>
<td>6%</td>
</tr>
<tr>
<td>Physical loss/non-electronic record</td>
<td>5%</td>
</tr>
</tbody>
</table>
What is business email compromise?

Business email compromise (BEC) is a social engineering attack in which a cybercriminal uses compromised email credentials or spoofs a legitimate email address in order to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by the cybercriminal or, in some cases, to transfer sensitive data such as W-2 forms. An email account takeover is a compromise of email account credentials through phishing or malware that allows a cybercriminal to access an email account and pose as the legitimate owner. Typically, the attacker sends a phishing email with a link to a website that looks legitimate and prompts the user to enter their username and password. On the backend, the attacker has now acquired those credentials.
How BEC has evolved?

Cybercriminals have moved beyond unsophisticated spam attacks and obvious phishing emails and are able to leverage and monetize a compromised email account in several ways.

1. **Reconnaissance and more effective spam**

One compromised account can allow an attacker to do reconnaissance and tailor the next phishing email in a way that will trick more users within the organization to give up credentials. Users are far more likely to click on a link in an email that was received from a legitimate sender or contains an official-looking banner. BBR Services regularly sees email compromise incidents involving multiple users, and sometimes over 100 users are compromised in a single, targeted phishing attack.

2. **Fraudulent wire transfers**

The attacker will search for and exploit an existing email chain regarding a forthcoming payment, request a change in wire instructions, and receive the funds in their own bank account. A few years ago, fraudulent transfers were typically under $15,000, but attackers have gotten bolder. BBR Services has seen a range of successful fraudulent transfers from several thousand dollars to seven figures. In the past year, the amounts stolen in this way have increased significantly as attackers get more brazen and successful. One promising development over the past year has been the banks’ ability to freeze the transaction and return the funds if they are contacted quickly enough (within 24-48 hours) by the targeted organization.

3. **Email as a launch point to other applications**

Bad actors sometimes begin their attack by compromising email inboxes, and then move into the HR/payroll self-service portal to change direct deposits. Attackers search the compromised inboxes to determine what portal the company uses, set up inbox forwarding rules to redirect any email from the portal directly to trash, reset the password for the portal if it wasn’t the same as for email, and then change the direct deposit to the attacker’s account. Often times users would not realize for one, two or even three pay periods that they were not receiving paychecks. If the organization uses Microsoft Office 365, the attack may also use the credentials to access OneDrive or other applications.

4. **Sensitive information in the inbox itself**

Attackers may steal sensitive information within the inbox. Such information could be used by the attacker or sold on the dark web.
BEC response challenges

Challenges in responding to BEC incidents are numerous, and BBR Services has guided hundreds of organizations through these issues. When responding to a BEC incident, organizations must closely examine affected email accounts and preserve evidence regarding how the attacker has specifically manipulated the accounts. Attackers may have created forwarding rules or used stolen credentials to access additional systems. Organizations should notify their carrier in order to retain data breach counsel and forensics support to review access logs and determine the extent to which whole accounts or only partial accounts are compromised.

If many emails, or whole email inboxes, are compromised, the forensic firm or an e-discovery vendor often must run programmatic keyword searches for sensitive information and potentially conduct a document review of the “hits” in order to put together a list of individuals whose personally identifiable information (PII) or protected health information (PHI) has been accessed or stolen. Among other logistical notification steps, organizations must compile a list of names and addresses for notification purposes, which can be challenging for an organization with older compromised data or that lack the ability to quickly identify current addresses.

Source: Ankura
Business email compromise continued

Office 365 business email compromise

A mortgage company was hit with a widespread phishing campaign involving an email with a link that took users to a website appearing to be a Microsoft Office 365 login page and directed them to enter their credentials. Based on our experience with the influx of Office 365 incidents, BBR Services recommended that the mortgage company work with privacy counsel and a forensic firm that has handled hundreds of similar attacks.

The forensic investigation revealed that over 100 users’ inboxes had been compromised in the attack, and because of the way in which the attacker accessed the inboxes, the forensic firm could not rule out the possibility that the attacker downloaded the entirety of each mailbox. In order for counsel and the company to determine if there was an obligation to notify affected clients, 900,000 files were programmatically searched for PII. The search hits required a document review of tens of thousands of files in order to identify affected individuals and create an address list. Ultimately, 60,000 clients or prospective clients were notified.

The legal fees, forensic costs, programmatic review, and document review alone cost nearly $2 million. The cost of notification, call center and credit monitoring was an additional $100,000.

Top 5 ways to prevent BEC

1. Implement multi-factor authentication for remote access to system and applications.
2. Provide regular anti-fraud training that teaches employees to detect and avoid phishing and social engineering scams.
3. For employees who frequently travel and are authorized to request funds transfers, establish a process to confirm requests. For example, set up a predetermined code that a request must include that is not documented within the network.
4. Limit the number of employees who have the authority to submit or approve wire transfers.
5. If a vendor or supplier requests changes to its account details (including, but not limited to, bank routing numbers, account numbers, telephone numbers, or contact information):
   - Confirm all requests by a direct call to the vendor or supplier. Use a phone number the vendor or supplier provided before the request was received.
   - Require review of all requests by a supervisor or next-level approver before making any changes.
   - Is the address or bank account to which the payment is to be sent different from previous payments to that vendor?
   - If the request is from a vendor, check for changes to business practices, such as whether earlier invoices were mailed while the new one was emailed or if earlier payments were by check and now the request is for a wire transfer.
   - Be suspicious of small changes in email addresses that mimic legitimate email addresses.
Ransomware

What is Ransomware?

Ransomware is a type of malicious software that restricts access to an infected machine, usually by systematically encrypting files on the system’s hard drive, and then demands payment of a ransom, usually in a cryptocurrency (e.g., Bitcoin), in exchange for the key or keys to decrypt the data.
How ransomware has evolved

In 2018, BBR Services encountered a wide range of ransomware incidents – many conducted by unskilled attackers through ransomware-as-a-service (RaaS) platforms, and others involving sophisticated attackers targeting specific organizations with a goal clearly beyond extortion. No organization is immune from the risk – cyber criminals attack organizations across all industries and sizes of business.

1. Organizations of all sizes and industries are targets, but small businesses that do not lockdown Remote Desktop Protocol (RDP) are at higher risk of being attacked.

The industries most impacted by ransomware are healthcare, financial services and professional services. Manufacturers have also been attacked with ransomware, and depending on how widely the ransomware spreads, some firms have to stop production for a period of time.

Small businesses were disproportionately hit by ransomware in 2018. In fact, 71% of the ransomware incidents reported to BBR Services impacted small businesses, which tend to spend less on information security and are more vulnerable. The main attack vector that cyber criminals used this year is RDP ports. Many small businesses outsource their IT to contractors that they allow to remotely access their networks via RDP. Attackers will scan the internet for open RDP ports, and then attempt to brute force a weak password to get access. Businesses that do not change the default RDP port, or who do not use strong passwords, are susceptible to this attack.

2. Attackers of varying skills use RaaS platforms to cast a wide net with minimal effort.

Using RaaS platforms available on the dark web, would-be cybercriminals can launch ransomware attacks more easily than ever. Less sophisticated attackers using RaaS create challenges for victims, including negotiations where the criminal simply disappears, decryption tools that corrupt files or don’t work at all, or criminals who cannot ensure successful decryption even after a ransom has been paid.

BBR Services also sees attackers employing sophisticated RaaS platforms. Recently, for example, attackers have made use of a payment portal that adjusts ransom demands for fluctuations in cryptocurrency valuations, charges a premium for using Bitcoin rather than the more anonymous Dash, and offers significant customer support for victims.

3. Attackers are using “sextortion” emails to trick victims into downloading ransomware.

Attackers also continue to launch ransomware through a tried and true attack vector – phishing emails. Phishing emails have become more convincing, and in some cases, more threatening. In one new type of attack, users receive an email from someone claiming to have accessed the recipient’s work computer and found the addresses of pornographic websites they have viewed. The sender says they have simultaneously recorded footage of the recipient as they watched these sites using their webcam, and threatens to share the files with their email contacts if demands are not met. The email contains a link or zip file they claim contains evidence of the internet or webcam activity, or to a website to pay the cryptocurrency ransom. But, if clicked on, the link may in fact spread malware that can steal information and install ransomware.

4. Larger organizations are still being targeted, and may receive higher ransom demands.

Though less common, BBR Services did receive reports throughout the year of sophisticated, targeted attacks, particularly by the Ryuk and SamSam hacking groups. These attack groups typically (though not always) go after larger organizations and because the attackers know what organization they have hit, the ransom demands are higher. BBR Services has dealt with cases involving multiple seven figure demands, the highest being $8.5 million or 3,000 Bitcoin. Fortunately, that organization did not have to pay the ransom and restored its data from backups. The highest ransom paid by a Beazley insured (and covered by Beazley) was just under $1 million. The average ransom demand was $116,324 (inflated because of the seven figure demands) and the median was $10,310.

5. Recently, BBR Services noticed an increase in ransomware attacks also involving banking Trojans.

Cyber criminals are now deploying banking Trojans to steal information, do reconnaissance, and launch ransomware. Banking Trojans are discussed in more detail below.
Ransomware response challenges

In addition to containing the ransomware virus and preserving forensics evidence, organizations face other challenges with ransomware, including understanding their ability to restore data from backups. If backups cannot be easily or quickly restored, organizations face the need to assess the pros and cons of paying the ransom demand. BBR Services has guided many organizations through these decisions and works with forensics vendors who are familiar with specific criminals’ behavior. Additionally, our forensics partners can assist with negotiating directly with the criminals, procuring cryptocurrency to pay the ransom and determining the likelihood that decryption methods will be reliable once the ransom is paid.

An additional challenge is that sometimes a ransomware attack is also a data breach. This depends on the attributes of the ransomware virus and whether access to or exfiltration of data occurred. In the healthcare sector, the Office for Civil Rights (OCR) has issued guidance that all ransomware attacks are presumed to be breaches unless there is a documented demonstration that PHI was not compromised or altered.
Ransomware continued

Six figure ransom demand

A leading construction and design firm with operations throughout the southern United States and in Mexico learned of a ransomware attack and received a $900,000 demand. The firm quickly learned its backups had been completely deleted. The insured saw no other option than to pay the ransom, and Beazley provided its consent for them to do so. Later, after an unknown person contacted the attacker and left an “insulting” message, the attacker demanded approximately $35,000 more, which the firm (with Beazley’s consent) paid. The firm paid a total of $935,000 in ransom payments and began decrypting its network. Beazley reimbursed the firm for almost $900,000 of the ransom payment. The manufacturer has also submitted data recovery and business interruption costs that amount to just over $1 million, though the claim is still being evaluated. BBR Services brought in privacy counsel and a forensic firm to investigate whether the attacker accessed or exfiltrated any sensitive personal information. Fortunately, the forensic firm determined no sensitive personal data was accessed by the attacker, and counsel determined that there was no notification obligation.

Top 5 ways to prevent ransomware

While many sophisticated ransomware attacks are occurring, by and large, we see attacks that come in through known vulnerabilities that could have been easily prevented. Below are the top five ways to prevent ransomware attacks against your organization.

1. Training
Run phishing campaigns to help employees recognize phishing attacks. Track the response rate and look out for repeat offenders.

2. Backups
Properly segment backups to prevent malware from spreading and infecting them.

3. Lock down RDP
Close down RDP ports, or if that cannot be done, enable multi-factor authentication on the port. Change the RDP port from the default port and use a strong password.

4. Multi-factor authentication
For any remote connection to the network or business applications, require a password and a second factor, typically a security code, making it more difficult for attackers to gain unauthorized access.

5. Patching and anti-virus
Allow automatic patching of the operating system and internet browsers. Stay on top of anti-virus software updates to detect new emerging threats which can go unnoticed in a system if the anti-virus program is out-of-date.
Banking Trojans

What are banking Trojans?

Banking Trojans are a form of malware originally designed to steal banking credentials, but recent variants such as Emotet and Trickbot have been enhanced by cybercriminals to harvest all types of account credentials. They also serve as a vehicle to deploy other malware.
How banking Trojans have evolved

Towards the end of 2018, BBR Services handled an increasing number of incidents involving banking Trojans.

1. Banking Trojans are becoming more dangerous and disruptive, and once infected, organizations may have a hard time eradicating them from their network.

An unsuspecting victim clicks a link in an email, downloading an infected file, or a file that prompts them to enable a feature that will then download malware onto the system. After installation, banking Trojans like Emotet and Trickbot are adept at disguising themselves and establishing persistence. Once they have infected one machine, banking Trojans spread aggressively through the network. They can harvest network credentials – network administrative credentials are especially valuable – and use them to attack other systems on the network. In some cases, users who have logged onto infected computers with admin credentials to try to mitigate the problem have actually caused it to spread further. The malware may also harvest any personal credentials entered or stored on the system.

2. Some banking Trojans can also exfiltrate emails from Outlook or serve as a precursor to a ransomware attack.

Stolen credentials aren’t the only information at risk. Some banking Trojans are able to exfiltrate emails from Outlook back to the attacker. When this occurs, a review of the emails may be necessary to determine whether any sensitive data was compromised. BBR Services has also managed incidents in which ransomware is deployed on systems following a successful banking Trojan infection. Sometimes the ransomware attack occurs immediately following the attack and other times the ransomware will be deployed months after the initial infection.

Banking Trojan response challenges

Banking Trojans can be particularly challenging because the longer they are in a system, the more they will hide themselves. BBR Services has seen instances where the initial response appears to have contained the infection, but the malware reappears soon thereafter. Organizations faced with a banking Trojan may need to work with forensics experts to contain the malware by deploying endpoint monitoring and may need to do a clean installation of the system once a forensics image is taken. Like other forms of attacks, consideration must also be given to whether a data breach has occurred depending on the properties and capabilities of the banking Trojan.
Banking Trojans continued

Retailer hit by banking Trojan

A major clothing retailer notified BBR Services that there had been an intrusion on their system. The company thought they had contained the intrusion. However, a month later the retailer contacted BBR Services again, stating malware was spreading across their network, and their outsourced IT firm was unable to contain the attack. The malware was causing downtime of their systems, resulting in an interruption to their business. BBR Services recommended a forensic firm well versed in banking Trojans as well as panel counsel. The forensic firm deployed endpoint monitoring and then worked with the retailer to contain and remove the malware from the system. The forensic investigation revealed that the banking Trojan detected more than a month prior had not been properly eradicated. Fortunately, the investigation also revealed that although the malware had spread across the network, it had not given the attacker access to sensitive personal information, nor did the attacker exfiltrate any such data. As such, counsel concluded no breach had occurred and no notification was required.

Top 5 ways to prevent banking Trojans

While anti-virus software can and certainly does prevent all kinds of attacks, the more sophisticated “zero day” banking Trojans will often elude anti-virus. The top five ways to prevent banking Trojans are:

1. Training
   Run phishing campaigns to help employees recognize phishing attacks. Track the response rate and look out for repeat offenders.

2. Lock down RDP
   Close down RDP ports, or if that cannot be done, enable multi-factor authentication on the port. Change the RDP port from the default port and use a strong password.

3. Multi-factor authentication
   For any remote connection to the network or business applications, require a password and a second factor, typically a security code, making it more difficult for attackers to gain unauthorized access.

4. Least Privilege Doctrine
   Banking Trojans thrive off of admin level credentials. By only providing users with the least amount of privileges that they need, organizations can help prevent further compromise of machines across the network.

5. Keep personal information off work computers
   Warn employees not to store any personal login information on their computers, even through their browsers.
The descriptions contained in this communication are for preliminary informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497).