Office 365 email compromises continue relentless rise

Attacks targeting business email accounts continued to climb in the second quarter, particularly for organizations using Office 365, the popular cloud-based productivity solution, according to newly released data from specialist insurer Beazley. Email compromises accounted for 23% of incidents reported to the Beazley Breach Response (BBR) Services team during the second quarter of 2018, up from 13% in the first quarter of the year. The attacks were broadly distributed across industry sectors, including healthcare, financial services, professional services and higher education.

Business email compromises are efficient for the hacker because the compromise of a single account gives the hacker a platform from which to spear phish within and outside the organization. While they can prove very expensive to a company that has been successfully attacked, they are also easily preventable. Indeed, the preventability of these attacks may be a red flag for regulators – BBR Services anticipates that regulators may look to make examples of organizations that are repeatedly hit.

In addition to securing a base for spear phishing attacks, attackers can also leverage compromised accounts to request fraudulent wire transfers, redirect an employee's payroll, and steal sensitive information within the inbox. According to Dasha Tarassenko of Mandiant, "Phishing emails coming out of the compromised accounts are becoming more targeted and impressively crafted than ever before. They're not just sending thousands of spam emails. They're doing reconnaissance within the compromised inbox and then tailoring the next phishing email to the recipient."

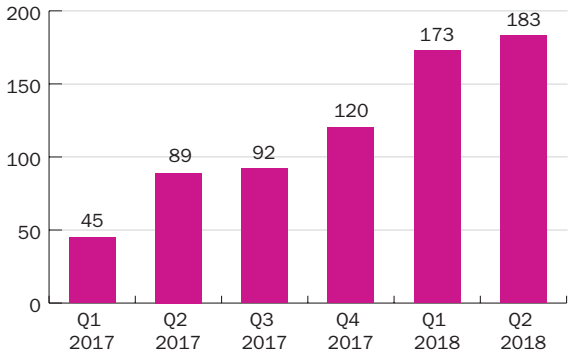
Tarassenko also explains that more sophisticated attackers may exploit PowerShell to log in to Office 365 and do more extensive reconnaissance. If they are able to compromise credentials for a user with the right administrative privileges, they may be able to search every single inbox for the entire organization.

These attacks are expensive because, in order for the target company to understand the full impact and whether personally identifiable information (PII) or protected health information (PHI) is at risk, they often require programmatic and manual searches of years' worth of emails for sensitive information. Unfortunately for the majority of organizations hit with this attack, more than one inbox is compromised. BBR Services often discovers that organizations are aware of only half the number of compromised inboxes. In some cases, there may actually be hundreds of inboxes compromised.

For larger scale email compromises, if the majority of users sent and received PII or PHI, the total cost of legal, forensics, data mining, manual review, notification, call center and credit monitoring can exceed $2 million. And even for the smaller scale email compromises, the costs can easily exceed $100,000.

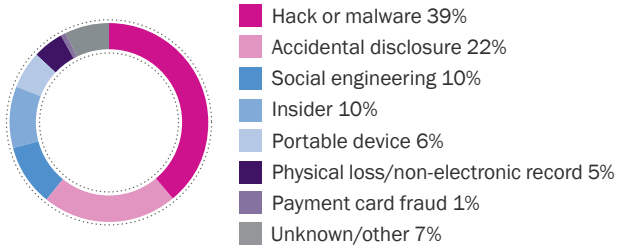
These attacks can easily be prevented by turning on two-factor authentication and training employees. Tarassenko also recommends disabling the ability for third-party applications to access Office 365, which can reduce the likelihood of an attacker using PowerShell for reconnaissance or other purposes.

Email compromises on the rise



The top two causes of data breaches reported to BBR Services in Q2 2018 were hack or malware attacks (39%) and accidental disclosure (22%). Hack or malware was down 3 percentage points from Q1, despite an increase in the number of email compromises. This is due to a slight decrease in the number of reported ransomware incidents in Q2.

Causes of incidents Q2 2018 (base 810)



CBSL565_US_07/18

Breaches by industry

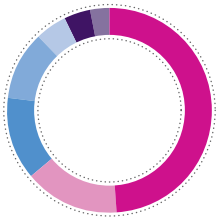
Higher education
Hack or malware incidents were down 4 percentage points from Q1 2018 to 43% of the total number of incidents for higher education institutions. While the number of reported hack or malware incidents did decrease slightly, this shift has more to do with the increase in other categories, such as insider and physical loss.

Financial services
49% of all data breach incidents reported to BBR Services in Q2 2018 were caused by hack or malware, down from 55% recorded in Q1. Similar to higher education, financial services entities reported an increase in insider incidents, which accounts for the shift in percentages.

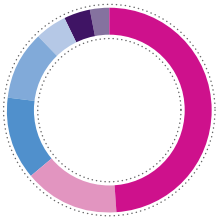
Healthcare
Accidental disclosure (38%) and hacking or malware (26%) endured as the most frequent causes of data breach in the healthcare sector in Q2 2018, at a combined 64% of the total. The number of accidental disclosure incidents increased from 29% in Q1 to 38% in Q2 because of an additional 24 reported incidents.

Professional services
Percentages remained largely unchanged for data breaches reported by professional services firms to BBR Services between Q1 and Q2 2018. The main change was a decrease in reported accidental disclosure incidents in Q2.

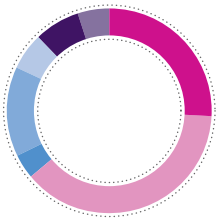
Higher Education Incidents, Q2 2018



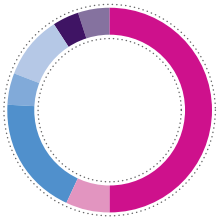
Financial Services Incidents, Q2 2018



Healthcare Incidents, Q2 2018



Professional Services Incidents, Q2 2018



Case study

A threat actor hit a health system with a widespread phishing campaign involving a phishing email with a link that took users to an official-looking website and directed them to enter their credentials. Based on its experience with the influx of Office 365 incidents, BBR Services recommended that the health system work with privacy counsel and a forensic firm that has handled hundreds of similar attacks on Office 365.

The forensic investigation revealed that approximately 20 users' inboxes were compromised in the attack, and because of the way in which the attacker accessed the inboxes, the forensic firm could not rule out that the attacker downloaded the entirety of each mailbox. In order for counsel and the health system to determine if there was an obligation to notify patients, the 20 inboxes were programmatically searched for PII and PHI. The search revealed upwards of 350,000 unsearchable documents, which were then manually reviewed by a vendor.

The legal fees, forensic costs, programmatic review, and manual review of documents alone cost just under $800,000. The cost of notification, call center and credit monitoring was an additional $150,000.

About Beazley's BBR Services Team

Beazley has managed thousands of data breaches since the launch of Beazley Breach Response in 2009 and is the only insurer with a dedicated in-house team focusing exclusively on helping clients handle data breaches.

The BBR Services team works directly with BBR insureds during all aspects of incident investigation and breach response and coordinates the expert services that BBR insureds need to satisfy legal requirements and maintain customer confidence. In addition to coordinating data breach response, BBR Services maintains and develops Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

beazley

www.beazley.com/bbr