TLP:WHITE

# Threat Intelligence Bulletin: Deloitte Breach

26 September 2017

This report, prepared by CyberInt, summarises the currently known information regarding the recent breach at Deloitte, one of the ‘big four’ accounting firms, and includes a timeline of events, what is known of the breach itself as well as the aftermath.

In addition to this summary, CyberInt are continuing to track this incident through the analysis of thousands of Darknet and Deep Web sources within the Argos™ threat intelligence platform. As well as monitoring for leakage of sensitive client data, CyberInt analysts are also observing closed source ‘chatter’ regarding this incident and will issue updates for any relevant findings.

The initial breach, believed to involve a compromised administrator account or accounts within Deloitte’s global email platform hosted on Microsoft’s Azure cloud, is reported as occurring during October or November of 2016 although it remained undiscovered until March 2017. Given this, the threat actor had effectively four to five months of potentially unrestricted access to the mailboxes of Deloitte’s 244,000 employees and any customer data contained therein.

## Key Points

- ‘Global’ email platform compromised with administrator account ‘access to all areas’;
- Estimated 5-million emails to/from Deloitte’s 244,000 employees potentially accessible along with attachments;
- Breach believed to be US-focused;
- Deloitte insisting that “only a small number of its clients had been impacted”;

## Timeline

Based on what has been revealed so far, the following key dates have been identified (Figure 1):

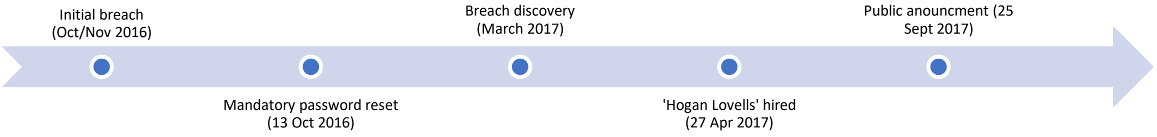

Initial breach (Oct/Nov 2016)
Mandatory password reset (13 Oct 2016)
Breach discovery (March 2017)
'Hogan Lovells' hired (27 Apr 2017)
Public anouncment (25 Sept 2017)

*Figure 1 - Deloitte breach timeline*

- October/November 2016 – Reported commencement of the breach;
  - Compromised administrator account(s);
  - Access to Deloitte’s global email infrastructure;
- 13 October 2016 – US-based Deloitte employees sent a ‘mandatory password reset’ email;
  - Email launched ‘Global Security Awareness week’;
  - Advised employees that their password would expire on 17 October 2016;
- March 2017 - Breach discovered by Deloitte;
  - Information limited to select senior partners and lawyers;
- 27 April 2017 – US (Washington-based) law firm ‘Hogan Lovells’ hired on a special assignment into a possible cybersecurity incident;

    - Retained to provide "legal advice and assistance to Deloitte LLP, the Deloitte Central Entities and other Deloitte Entities";
- 25 September 2017 – Public announcement;
    - Undiscovered for around five months and publicly revealed six months later;
    - Following any public data breach announcement, security researchers and threat actors alike will undoubtedly search for further details and any exposed data;

## Breach

Based on the information currently available, the initial breach in October or November 2016 involved the compromise of an administrator account or accounts resulting in unauthorised and reportedly unrestricted access to Deloitte's email platform. This 'Global' email platform, hosted within Microsoft's Azure cloud, is thought to contain the mailboxes of 244,000 Deloitte employees along with some estimated 5-million emails of which potentially sensitive content and attachments could include usernames, password and architectural or design documentation for both Deloitte and their clients.

The nature of how, and exactly when, the breach occurred has not fully been revealed so far, likely due to ongoing investigations. Given this, the subsequent 'mandatory password reset' notification reportedly sent to US-based employees around the time of the breach may be unrelated and cannot necessarily be confirmed as an indication of Deloitte being aware earlier than reported. Initial reports suggest that Deloitte became aware of the potential breach in March 2017 and subsequently hired US-based law firm 'Hogan Lovells' with regards to a "possible cybersecurity incident", retaining their "legal advice and assistance" services presumably throughout the disclosure and ramifications of the attack.

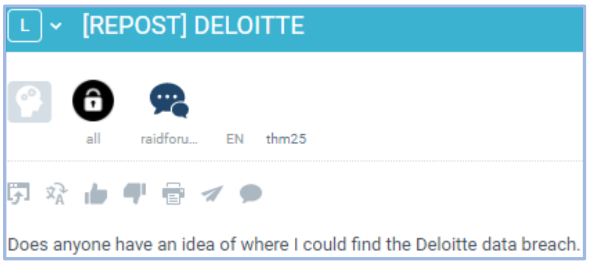
Furthermore, it is currently understood that the attack and breach focused on US-based content, including 'household names as well as US government departments' with a source speaking to 'Krebs on Security'[1] suggesting that the investigation, codenamed 'Windham', was focused on a Deloitte office known as the 'Hermitage' based in Nashville, US.

Deloitte have subsequently issued a statement to 'Krebs on Security' regarding this "cyber incident" and have down-played the scale of the intrusion as impacting "very few clients" with "no disruption to client businesses, to Deloitte's ability to continue to server clients, or to consumers". The Guardian reports that Deloitte has contacted six impacted clients, as well as notifying government authorities and regulators, although no public confirmation or date of notification has been published.

[1] https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

## Aftermath

Following any breach announcement, cyber security professionals and threat actors alike will often seek more information about the attack as well as any potentially leaked data. In this instance, Argos™, CyberInt's Threat Intelligence Platform, alerted analysts to chatter regarding this incident (Figure 2).



[REPOST] DELOITTE

Does anyone have an idea of where I could find the Deloitte data breach.

*Figure 2 – CyberInt Argos™ alert following the Deloitte breach announcement*

## Discussion Points

Whilst it is too early to fully understand the nature of this breach, some learning or discussion points should be considered:

- Robust password security/policy;
    - Was this breach due to password reuse, a potentially weak password or password policy allowing it to be brute-forced or guessed? These factors continue to be leveraged by threat actors.
- Multi-factor authentication;
    - Were the administrator accounts protected with multi-factor authentication in order to bolster their security? Combining something you know (a password) with something you have (a hardware or software token) and something you are (biometrics) increases the complexity for threat actors. Deloitte themselves suggest that "MFA should be considered a priority for organizations"[2].
- Data encryption;
    - If emails and attachments are encrypted, the impacts of a breach may be mitigated by a threat actors inability to compromise multiple encryption keys.

[2] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-deloitte-multi-factor-authentication.pdf