Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

Cybersecurity Alert

TLP:GREEN

Cybersecurity landscape is changing.
Hospitality industry needs to be aware of POC malware and "third party" or "Supply-Chain" attacks.
Business entities in Hong Kong should perform security risk assessment on their outsourced IT operations.
Attacks can also be caused by insiders.

On Dec 10, 2018, a blog on KrebsOnSecurity attracted our attention: "We don't yet know the root cause(s) that forced *Marriott*[1] this week to disclose a four-year-long breach involving the personal and financial information of 500 million guests of its *Starwood hotel* properties".

This is another mega Personal Identifiable Information (PII) breach being announced ever since the EU's General Data Protection Regulation (GDPR)[2] comes into full effect on May 25, 2018. As per the announcement made by Marriott[3] on Nov 30, 2018, the unauthorized access to the Starwood guest reservation database in the United States happened on or before Sept 10, 2018, but an internal investigation found that an attacker had been able to access the Starwood network with Point-of-Sales (POS) malware[4] since 2014, and Marriott bought Starwood in 2016[5].

We have no way, and no interest, to investigate why "an old story" was put on the table again as Starwood had already disclosed the breach in Nov 2015[6]. However, similar to *our recent Cathay Pacific data breach incident*, even though leading security experts were quickly engaged to investigate what occurred, it still needs a lengthy time to decrypt the information and determine what contents were being accessed by the attacker(s). As a Hong Kong based cybersecurity consulting firm, our focus are put back to Hong Kong. We digged out another past incident dated back in 2015 where the luxury hotel chain *Mandarin Oriental* [7]was hitted by the similar POS credit card heist.[8] Mandarin did not mention how many of their hotels were impacted, but the card information was believed to have been stolen from compromised payment terminals[9] at restaurants and gift shops within the affected hotels.

Last week we attended a webinar conducted by Flashpoint on the topic of "Exploring Asia Pacific's Cybercrime Landscape". The analyst from Flashpoint discussed PII breaches, carding and cashing incidents in APAC regions. They have also mentioned a case that compromised data belonging to a

[1] Marriott: Data on 500 Million Guests Stolen in 4-Year Breach. https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/
[2] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[3] http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
[4] https://www.zdnet.com/article/marriott-announces-data-breach-affecting-500-million-hotel-guests/
[5] https://www.bbc.co.uk/news/amp/technology-46401890?__twitter_impression=true and https://www.zdnet.com/article/starwood-hotels-fall-prey-to-point-of-sale-malware/
[6] https://krebsonsecurity.com/2015/11/starwood-hotels-warns-of-credit-card-breach/
[7] https://www.mandarinoriental.com/media/press-releases/statement-relating-to-credit-card-breach.aspx
[8] https://hacked.com/mandarin-oriental-hotel-chain-hacked/
[9] https://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

Chinese hotel chain[10] was available for sale on Aug 28, 2018 in Chinese dark webs, and also on unsupervised Telegram channels. According to the hacker's posting, the stolen data is of 141.5GB in size, containing 240 million records on roughly 130 million hotel guests that have stayed at hotels which are managed by Huazhu, including brands such as – Hanting Hotel, Grand Mercure, Joye, Manxin, Novotel, Mercure, CitiGo, Orange, All Season, Starway, Ibis, Elan, Haiyou (Refer to Fig 1). Unlike the previously discussed cases, this is called a *third-party* or *supply chain* attack as *an insider* [11] posted the hotel's CMS (Customer Management System) source code, root ID and password onto GitHub (Refer to Fig. 2).

Fig 1 – Compromised data belonging to a Chinese hotel chain was available for sale in Chinese dark webs

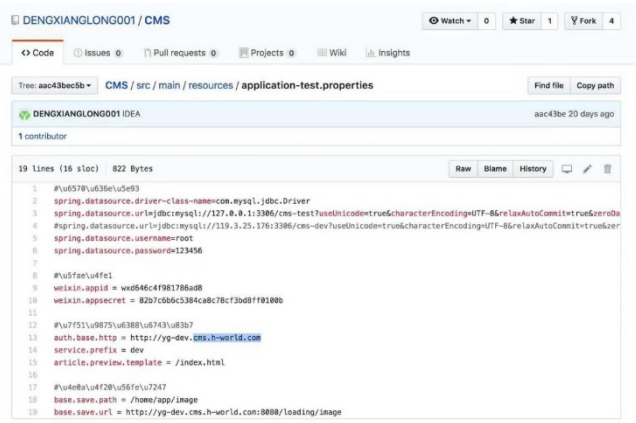

Fig 2 – Hotel's CMS source code, root ID, and password, were posted onto GitHub

Based on the identified TTPs (Tactics, Techniques, and Procedures), we performed a search on GitHub and found an almost-identical leak that are related to a few organizations, including banks and IT company in Hong Kong. We immediately informed one of the affected organizations and told them that the source code and test database (not involving card data) are on GitHub which could allow attackers to launch cyberattacks against them and may cause further data breach (Refer to Fig 3). We believed that the source code and test database were leaked by mistakes from a careless employee of an out-sourced contractor.

All of these incidents indicated that the cybersecurity landscape is shifting from US, Europe to APAC region including Hong Kong. Implementing network and end-point base security solutions alone are no longer sufficient to protect enterprise/organizations in Hong Kong.

We have to pay more attentions on the *third-party* or *supply chain* attacks[12].

"IT CAN HAPPEN TO ANYONE AND IT MAY HAPPEN AGAIN"

[10] https://www.bleepingcomputer.com/news/security/data-of-130-million-chinese-hotel-chain-guests-sold-on-dark-web-forum/
[11] https://wallstreetcn.com/articles/3396526
[12] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjX1MqArZvfAhWKjLwKHQAgAdMQFjAAegQIChAC&url=https%3A%2F%2Fwww.nist.gov%2Fdocument-87&usg=AOvVaw1IU39FjxO018VsuLBaqBFc

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

```
function EngineerWebForm(){

                                        //$receiver = "[redacted]@[redacted]com.hk";
                                        $receiver = explode(";", $_POST['to']);
                                        $cc = explode(";", $_POST['cc']);

                                        $arr = array(   "[redacted]To" => "[redacted].to@[redacted].hk"
                                                        ,"[redacted]au" => "[redacted].lau@[redacted].hk"
                                                        ,"[redacted]Ko" => "[redacted].ko@[redacted].hk"
                                                        ,"[redacted]Sin" => "[redacted].sin@[redacted].hk"
                                                        ,"[redacted]Yip" => "[redacted].yip@[redacted].hk");
                                        foreach($arr as $k => $v){
                                                if($v == $_POST['enter_by']){
                                                        $enter_by = $k;
                                                }

                                        }

                                        require_once(APP_INC_PATH . "phpmail/class.phpmailer.php");
                                        $mail = new PHPMailer();
                                        $mail->IsSMTP(); // send via SMTP
                                        $mail->Host = "[redacted].com.hk"; // SMTP servers
                                        $mail->SMTPAuth = true; // turn on SMTP authentication
                                        $mail->Username = "[redacted]"; // SMTP username
                                        $mail->Password = "[redacted]"; // SMTP password
                                        $mail->CharSet = "utf-8";
                                        $mail->From = "[redacted].com";
                                        $mail->FromName = "BreakFix_Request";
```

```
21          function core($receiver, $cc, $subject, $body, $attachment = null, $image = null){
22                                      $receiver = explode(";", $receiver);
23                                      $cc = explode(";", $cc);
24
25                                      require_once(APP_INC_PATH . "phpmail/class.phpmailer.php");
26                                      $mail = new PHPMailer();
27                                      $mail->IsSMTP(); // send via SMTP
28                                      $mail->Host = "mail.[redacted].com.hk"; // SMTP servers
29                                      $mail->SMTPAuth = true; // turn on SMTP authentication
30                                      $mail->Username = "[redacted]"; // SMTP username
31                                      $mail->Password = "[redacted]"; // SMTP password
32                                      $mail->CharSet = "utf-8";
33                                      $mail->From = "[redacted].com";
34                                      $mail->FromName = "[redacted] Service Desk";
35                                      $mail->AddReplyTo("[redacted].com","[redacted]Service Desk");
36                                      // 執行 $mail->AddAddress() 加入收件者，可以多個收件者
37
38                                      for($i=0; $i<count($receiver); $i++){
39                                              $mail->AddAddress($receiver[$i]);
40                                      }
41
42                                      //$mail->AddAddress("to2@email.com"); // optional name
43                                      if($cc != null){
44                                              for($i=0; $i<count($cc); $i++){
45                                                      $mail->AddCC($cc[$i]);
46                                              }
47                                      }
```

Fig 3 – Leaked Source code, emails and test ID/passwords of a Hong Kong organization on GitHub