Ousaban: Private photo collection hidden in a CABinet

welivesecurity.com/2021/05/05/ousaban-private-photo-collection-hidden-cabinet/

May 5, 2021

Another in our occasional series demystifying Latin American banking trojans

ESET Research
5 May 2021 - 11:30AM

Another in our occasional series demystifying Latin American banking trojans

Ousaban is a Latin American banking trojan active exclusively in Brazil. ESET has been tracking this malware family since 2018. In common with most other LATAM banking trojans, Ousaban uses overlay windows to steal credentials and more from financial institutions. However, unlike most other LATAM banking trojans, Ousaban's developers have extended the use of overlay windows to steal credentials from popular regional email services. In this installment of our series, we examine its main features and many connections to other Latin American banking trojan families.

Characteristics

Ousaban is written in Delphi, as are the vast majority of the other Latin American banking trojans ESET is tracking. And, as do many of them, Ousaban shows signs of active and continuous development.

The name ESET assigned to this family is a portmanteau of two words – “**ousa**dia”, which means “boldness” in Portuguese, and “**ban**king trojan”. The reason for such a name is that for a very long time, Ousaban was distributed alongside the images (some of them obscene) shown in Figure 1. In the most recent campaigns distributing Ousaban, this is no longer the case.

Figure 1. Various images distributed alongside the Ousaban banking trojan

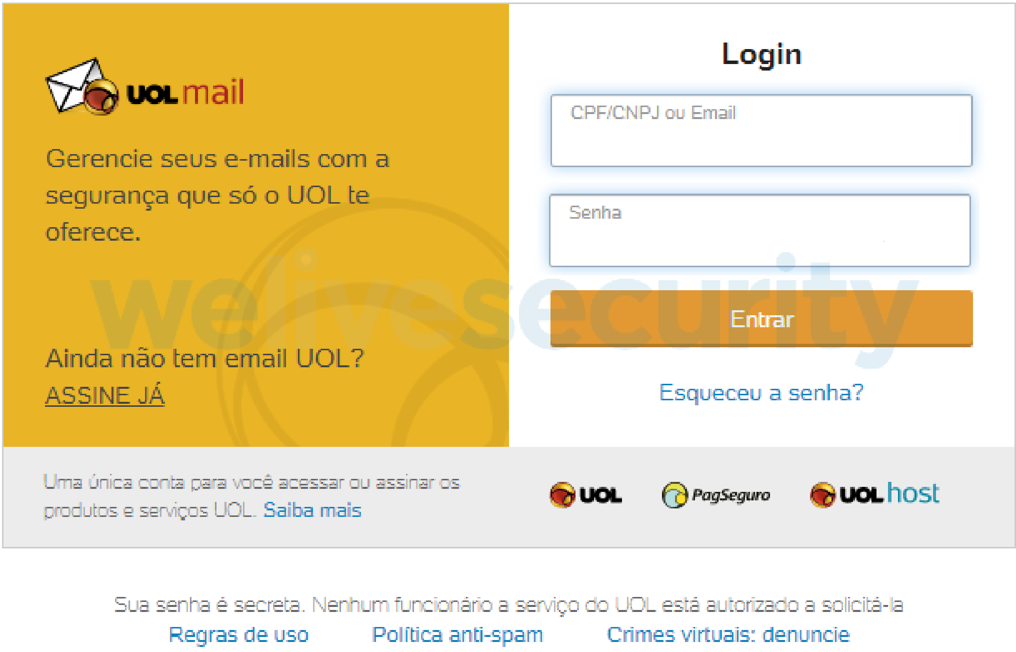
Ousaban is also known as Javali, a name assigned by Kaspersky. A recent article about Ousaban can be found here. ESET has also been able to attribute Ousaban to the campaigns described in this blogpost from 2018. Even though some sources claim Ousaban is active in Europe, ESET has never observed any campaign spreading this banking trojan outside of Brazil.

Ousaban protects its executables with either Themida or Enigma binary obfuscators. Additionally, most EXEs are enlarged, using binary padding, to approximately 400 MB, likely in order to evade detection and automated processing.

Most recent Ousaban variants contain a string table to hold their strings, storing this table in their .rsrc sections. One of the resources contains a zlib-compressed list of strings delimited by newline characters.

Its backdoor capabilities are very similar to a typical Latin American banking trojan – simulating mouse and keyboard actions and logging keystrokes. The latest variants communicate with C&C servers using RealThinClient – a protocol also used by Grandoreiro.

The typical Latin American banking trojan attacks users of financial institutions using overlay windows crafted specifically for its targets and Ousaban is no exception. Interestingly though, its targets include several email services that it has overlay windows ready for as well, as illustrated in Figure 2.



Gerencie seus e-mails com a segurança que só o UOL te oferece.

Ainda não tem email UOL?
ASSINE JÁ

Login

CPF/CNPJ ou Email

Senha

Uma única conta para você acessar ou assinar os produtos e serviços UOL. Saiba mais

Sua senha é secreta. Nenhum funcionário a serviço do UOL está autorizado a solicitá-la

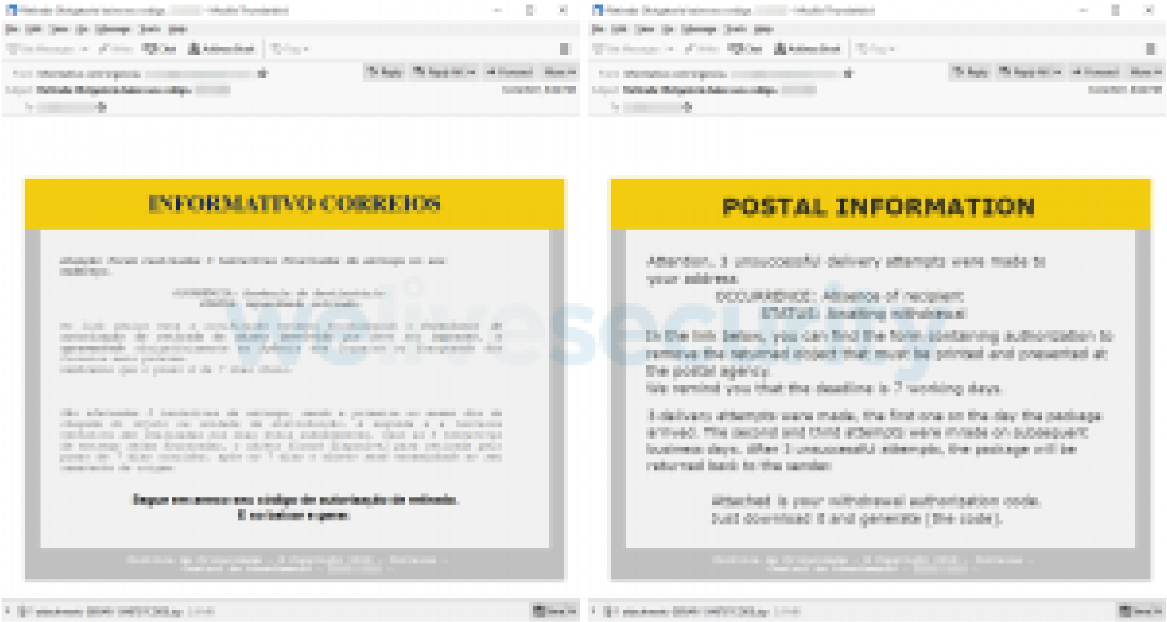
Figure 2. Overlay window design for the UOL email service

To achieve persistence, Ousaban either creates a LNK file or a simple VBS loader in the startup folder, or it modifies the Windows registry Run key.

Distribution and execution

Ousaban is distributed mainly through phishing emails (such as the one in Figure 3). The threat actor behind Ousaban cycles through multiple distribution chains. These chains share some common characteristics, mainly:

- DLL side-loading is used to execute a binary payload
- CAB archives are sometimes used instead of ZIP
- A configuration file distributed inside an archive with one stage is required by the next stage
- An injector, unique to Ousaban, may be used



INFORMATIVO CORREIOS

[illegible]

Segue em anexo seu código de autorização de retirada.
É só baixar e gerar.

POSTAL INFORMATION

Attention, 3 unsuccessful delivery attempts were made to your address.

OCCURRENCE: Absence of recipient
STATUS: Awaiting withdrawal

In the link below, you can find the form containing authorization to remove the returned object that must be printed and presented at the postal agency.
We remind you that the deadline is 7 working days.

3 delivery attempts were made, the first one on the day the package arrived. The second and third attempts were made on subsequent business days. After 3 unsuccessful attempts, the package will be returned back to the sender.

Attached is your withdrawal authorization code.
Just download it and generate [the code].

Figure 3. Recent spam email distributing Ousaban (a rough translation is provided on the right)

MSI with JavaScript

This distribution chain, illustrated in Figure 4, is quite straightforward. The victim is misled into executing an MSI attached to the phishing email. When executed, the MSI launches an embedded JavaScript downloader that downloads a ZIP archive and extracts its contents. It then executes the legitimate application, which side-loads the Ousaban banking trojan.

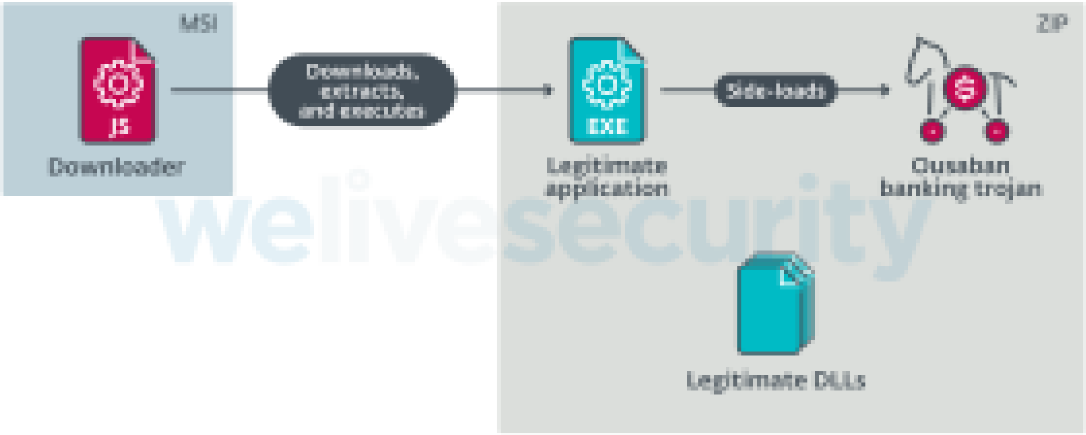


Figure 4. Simple Ousaban distribution chain

Multistage MSI

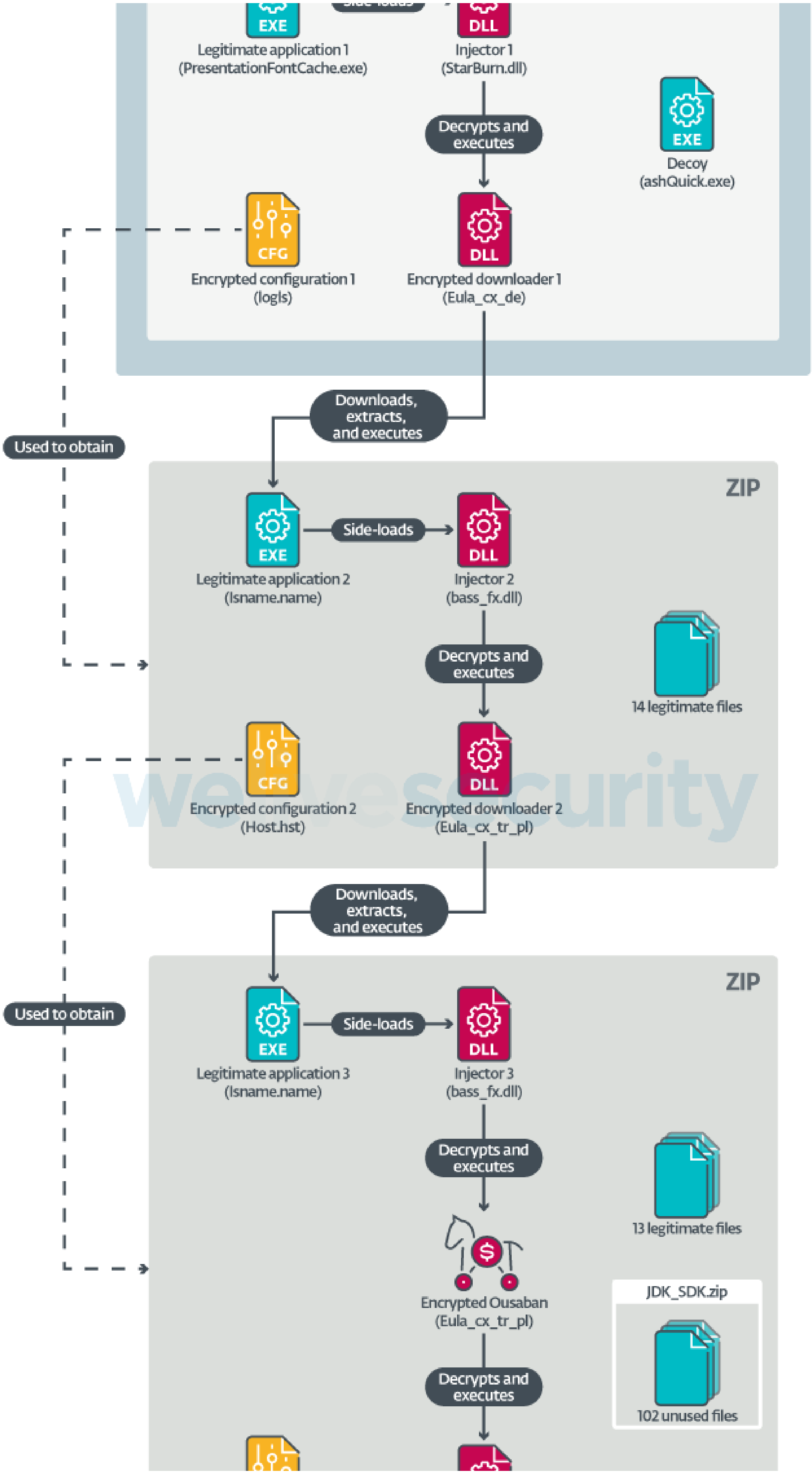
Recently, ESET has observed a new distribution chain spreading Ousaban massively. It is much more complicated than the one described above. The whole process is illustrated in Figure 5.

The first two stages are almost identical. In both, the core of the stage is contained in an archive (ZIP or CAB) and contains:

- A legitimate application
- An encrypted injector
- An encrypted downloader
- An encrypted configuration file
- Legitimate files

The legitimate application, when executed, side-loads the injector. The injector locates, decrypts and executes the downloader. The downloader decrypts the configuration file to obtain a URL leading to a remote configuration. The remote configuration contains a URL leading to the next stage archive. The downloader downloads the next stage archive, extracts its contents and executes the legitimate application.

The final stage is slightly different, as it decrypts and executes the actual Ousaban banking trojan instead of a downloader. The third configuration file leads to a remote configuration with C&C server IP address and port. The archive with the last stage contains one more malware-related file – a support module that alters various settings of the victim’s machine. Finally, the archives for all three stages include additional files – a single legitimate executable in the first-stage archive, 14 legitimate files in the second-stage archive, and 13 legitimate files in the third-stage archive plus an embedded archive containing a further 102 legitimate files.


EXE
Legitimate application 1
(PresentationFontCache.exe)
DLL
Injector 1
(StarBurn.dll)
Decrypts and executes
EXE
Decoy
(ashQuick.exe)
CFG
Encrypted configuration 1
(logls)
DLL
Encrypted downloader 1
(Eula_cx_de)
Downloads, extracts, and executes
Used to obtain
ZIP
EXE
Legitimate application 2
(lsname.name)
Side-loads
DLL
Injector 2
(bass_fx.dll)
Decrypts and executes
14 legitimate files
CFG
Encrypted configuration 2
(Host.hst)
DLL
Encrypted downloader 2
(Eula_cx_tr_pl)
Downloads, extracts, and executes
Used to obtain
ZIP
EXE
Legitimate application 3
(lsname.name)
Side-loads
DLL
Injector 3
(bass_fx.dll)
Decrypts and executes
13 legitimate files
Encrypted Ousaban
(Eula_cx_tr_pl)
JDK_SDK.zip
102 unused files
Decrypts and executes

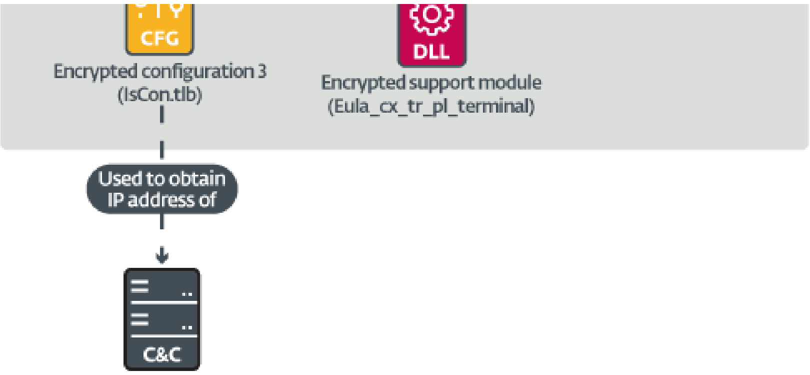


Figure 5. Ousaban's complex distribution chain

Support module

Ousaban loads this module to make it easier for the threat actor to connect to the victim's machine. It mainly:

- Modifies the RDP settings to use RDPWrap, a utility to allow multiple RDP connections to Home editions of the Windows OS
- Modifies firewall settings to allow all RDP connections
- Creates a new account with administrative privileges

The module contains the RDPWrap binaries stored in its .rsrc section. It then changes the RDP settings directly in the Windows registry at:

- HKLM\SYSTEM\CurrentControlSet\Services\TermService\
- HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\

The module then uses netsh.exe to modify the Windows firewall to allow all TCP and UDP traffic directed to port 3389, the standard port for RDP. Finally, it creates a new account Administrat0r with administrative privileges. We hypothesize that the threat actor wants to have a second way to access the victim's machine; the threat actor is then not limited by the capabilities of the Ousaban banking trojan and can perform any malicious activity.

Cryptography

Ousaban utilizes three cryptographic schemes overall. Its strings are encrypted with an algorithm used by the vast majority of Latin American banking trojans we have analyzed (we have previously described it in detail here). All communications between Ousaban and its C&C server are encrypted using the standard AES cipher with a hardcoded key.

The final algorithm is used in the previously mentioned injector specific to this family. We provide a Python implementation in Figure 6.

```
def decrypt(data, key):
data_dec = str()
key_len = len(key)
for i, c in enumerate(data):
if i % 2 != 0:
data_dec += chr(key[i % key_len ^ c ^ ((key_len - (i & key_len)) & 0xFF)])
else
data_dec += chr(key[i % key_len] ^ c ^ (i & 0xFF))

return data_dec
```

Figure 6. Algorithm used by Ousaban's injector to decrypt its payloads

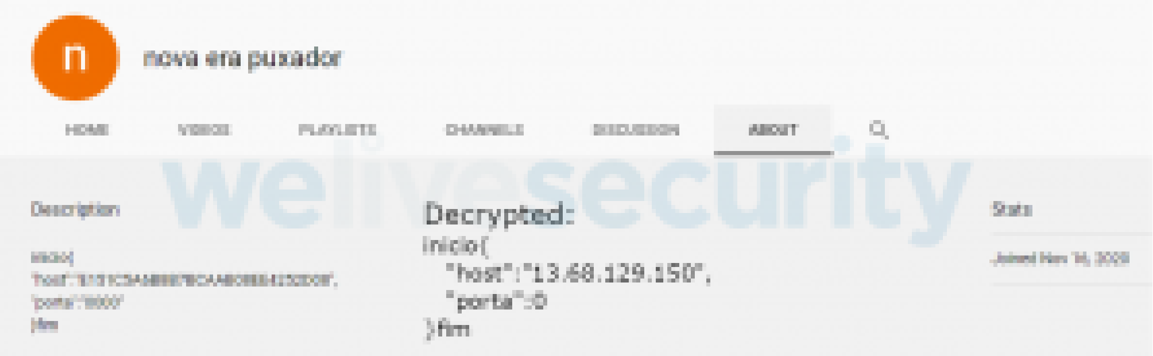
Remote configuration

Ousaban relies on remote configuration to obtain its next stage URLs and the C&C address and port to use. Ousaban used to store its remote configuration on YouTube, similar to Casbaneiro, but lately it has started using Google Docs instead.

The remote configuration is in JSON format with the values being encrypted by the same algorithm used for strings, but with a different key. The fields have the following meaning:

- host = C&C domain
- link = next stage URL
- porta = C&C port or 0 (the default HTTP port 80 is then used)
- vers = Ousaban version

Examples of the remote configuration are provided in Figure 7 and Figure 8.

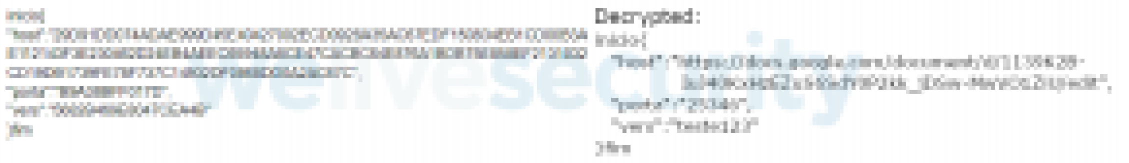


```
inicio{
"host":"[illegible]",
"porta":"[illegible]"
}fim
```

Decrypted:

```
inicio{
  "host":"13.68.129.150",
  "porta":0
}fim
```

Figure 7. Ousaban remote configuration on YouTube



```
inicio{
"host":"[illegible]",
"porta":"[illegible]",
"vers":"[illegible]"
}fim
```

Decrypted:

```
inicio{
  "host":"https://docs.google.com/document/d/[illegible]",
  "porta":"25340",
  "vers":"teste123"
}fim
```

Figure 8. Ousaban remote configuration on Google Docs

Similarities with other LATAM banking trojans

We have already mentioned some similarities between Ousaban and other Latin American banking trojans previously analyzed in this series (like the same string decryption algorithm). During our analysis, we discovered additional links to the other families, mainly:

- Some Ousaban downloaders contain the same string obfuscation code as Amavaldo
- Ousaban has been distributed by the same malicious advertisements as Mispadu in the past
- The JavaScript files it uses are similar to Vadokrist, Mekotio, Casbaneiro and Guildma
- The PowerShell files it occasionally uses for distribution (aside from the recent methods described in this blogpost) are similar to Amavaldo, Casbaneiro and Mekotio

We analyzed the interestingly close cooperation between these malware families in depth in our white paper presented at the Virus Bulletin 2020 conference.

Conclusion

In this installment of our series, we looked at Ousaban, a Latin American banking trojan targeting only Brazil. This malware family has been active since at least 2018 and shares typical characteristics of this type of threat – it is written in Delphi, contains backdoor functionality and attacks using overlay windows.

We have covered its most typical features, distribution and execution methods and the structure of its remote configuration. We also discovered several leads that suggest Ousaban is linked to some other Latin American banking trojans.

For any inquiries, contact us at threatintel@eset.com. Indicators of Compromise can also be found in our GitHub repository.

Indicators of Compromise (IoCs)

Hashes

SHA-1	Description	ESET detection name
C52BC5B0BDFC7D4C60DF60E88835E3145F7FB34F	Ousaban banking trojan	Win32/Spy.Ousaban.G
D04ACFAF74861DDC3B12E75658863DA65C03013F	Ousaban JS downloader	JS/TrojanDownloader.Banload.AAP
9A6A4BF3B6E974E367982E5395702AFF8684D500	Ousaban JS downloader	JS/TrojanDownloader.Banload.AAP
3E8A0B6400F2D02B6B8CD917C279EA1388494182	Ousaban MSI downloader	Win32/Spy.Ousaban.W
6946BFB8A519FED8EC8C30D9A56619F4E2525BEA	Ousaban injector	Win32/Spy.Ousaban.W
E5DD2355E85B90D2D648B96C90676604A5C3AE48	Ousaban support module	Win32/Spy.Ousaban.AB

Abused legitimate applications

Example SHA-1	EXE name	DLL name
BA5493B08354AEE85151B7BBD15150A1C3F03D1D	Avira.SystrayStartTrigger.exe	Avira.OE.NativeCore.dll
7F6C820B00FC8C628E2420C388BBB9096A547DAA	AudioGrabber.exe	StarBurn.dll
C5D5CF1B591C40344B20370C5EE5275356D312EC	PlGen.exe	bass_fx.dll
53045B8047CED049BBC7EBCB3D3299D2C465E8B9	BlazeDVD.exe	SkinScrollBar.dll
A6118D354D512DC29965E368F6C78AA3A42A27AD	ImageGrabber.exe	StarBurn.dll
F9C71277CF05738275261D60A9E938CBA7232E0D	nvsmartmaxapp.exe	nvsmartmax.dll

Recent configuration file URLs

https://docs.google[.]com/document/d/1o9MlOhxIJq9tMOuUHJiw2eprQ-BGCA_ERnbF54dZ25w/edit
https://docs.google[.]com/document/d/1nQqifeYFsCcI7m-L1Y1oErkp50c-y670nfk7NTKOztg/edit
https://docs.google[.]com/document/d/13A6EBLMOOdvSL3u6IfyrPWbYREXNRVdDTiKzC6ZQx7U/edit
https://docs.google[.]com/document/d/1UiuqrzI_rrtsJQHqeSkp0sexhwU_VSje8AwS-U6KBPk/edit
https://docs.google[.]com/document/d/1VKxF3yKbwQZive-ZPCA4dAU1zOnZutJxY2XZA0YHa3M/edit
https://docs.google[.]com/document/d/19bXTaiFdY5iUqUWXl92Js7i9RoZSLJqcECgpp_4Kda4/edit
https://docs.google[.]com/document/d/1DDDmJzBVcNWhuj8JMRUVb7JlrVZ5kYBugR_INSS96No/edit
https://docs.google[.]com/document/d/1UbfOcHm-T9GCPiitqDRh5TNwZRNJ8_miEpLW-2ypU-I/edit
https://docs.google[.]com/document/d/1d1903AvDBYgOo0Pt9xBBnpCHwSerOpIi4l1b6M4mbT4/edit
https://docs.google[.]com/document/d/1JLuJKoxcd0vRqut8UeBjFJXzMDQ9OiY2ItoVIRq6Gw8/edit
https://docs.google[.]com/document/d/1EOwVDlYPV3gE7PSnLZvuTgUQXvOSN9alyN5aMw7bGeI/edit
https://docs.google[.]com/document/d/18sc6rZjk529iYF2iBTsmuNXvqDqTBSH45DhSZpuLv_U/edit

MITRE ATT&CK techniques

Note: This table was built using version 8 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Ousaban operators register domains to be used as C&C servers.
T1587.001	Develop Capabilities: Malware	Ousaban is operated by the same group that develops it.	
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Ousaban's initial downloader is most commonly distributed as a spam attachment.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	Ousaban uses PowerShell in some distribution chains.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Ousaban uses the cmd.exe to execute the legitimate applications that side-load the main Ousaban payload.	
T1059.007	Command and Scripting Interpreter: JavaScript/JScript	Ousaban uses JavaScript in some distribution chains.	

Tactic	ID	Name	Description
T1204.002	User Execution: Malicious File	Ousaban relies on the victim to execute the distributed MSI file.	
Persistence	T1098	Account Manipulation	Ousaban registers a new local administrator account on the victim’s machine.
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Ousaban achieves persistence using the Run key or startup folder.	
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Ousaban payloads and strings are encrypted.
T1574.002	Hijack Execution Flow: DLL Side-Loading	Ousaban is often executed by this technique.	
T1562.001	Impair Defenses: Disable or Modify Tools	Ousaban modifies the RDP settings of the victim’s machine.	
T1562.004	Impair Defenses: Disable or Modify System Firewall	Ousaban modifies Windows firewall settings.	
T1027.001	Obfuscated Files or Information: Binary Padding	Ousaban frequently uses binary padding.	
T1027.002	Obfuscated Files or Information: Software Packing	Ousaban binaries are protected by Themida or Enigma packers.	
T1218.007	Signed Binary Proxy Execution: Msiexec	Ousaban uses the MSI format for execution.	
Credential Access	T1056.001	Input Capture: Keylogging	Ousaban can capture keystrokes.
Discovery	T1010	Application Window Discovery	Ousaban looks for bank- and email-related windows based on their window names and titles.
T1518.001	Software Discovery: Security Software Discovery	Ousaban collects information about the security software installed on the victim’s machine.	
T1082	System Information Discovery	Ousaban collects basic information about the victim’s machine, such as computer name and Windows version.	
T1113	Screen Capture	Ousaban can take screenshots.	
Command and Control	T1132.002	Data Encoding: Non-Standard Encoding	Ousaban uses RealThinClient that provides non-standard encryption.

Tactic	ID	Name	Description
T1219	Remote Access Software	Ousaban installs RDPWrap on the victim’s machine.	
Exfiltration	T1041	Exfiltration Over C2 Channel	Ousaban exfiltrates data via C&C server.

5 May 2021 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion