


taskmgr.exe 

malicious

This report is generated from a file or URL submitted to this webservice on October 9th 2017 20:10:46 (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: 100/100

AV Detection: 93%

Labeled as: [Trojan.Generic](#)

[#njrat](#) [#rat](#)

Overview

Sample unavailable

Downloads

External Reports

Re-analyze


Looking for file context ...

Looking for similar samples ...

Report False-Positive

Request Report Deletion

Incident Response

 Risk Assessment

Remote Access

Persistence

Fingerprint

Evasive

Network Behavior

Uses network protocols on unusual ports

Creates a fake system process

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

Modifies firewall settings

Writes data to a remote process

Reads the active computer name


Reads the cryptographic machine GUID

Tries to sleep for a long time (more than two minutes)

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.



| | |
|---|----|
| Anti-Detection/Stealthyness | |
| Creates a fake system process | ▼ |
| External Systems | |
| Sample was identified as malicious by a large number of Antivirus engines | ▼ |
| Sample was identified as malicious by at least one Antivirus engine | ▼ |
| General | |
| The analysis extracted a file that was identified as malicious | ▼ |
| The analysis spawned a process that was identified as malicious | ▼ |
| Installation/Persistence | |
| Writes data to a remote process | ▼ |
| Network Related | |
| Uses network protocols on unusual ports | ▼ |
| Pattern Matching | |
| YARA signature match | ▼ |
| System Security | |
| Modifies firewall settings | ▼ |
| Hiding 1 Malicious Indicators | |
| All indicators are available only in the private webinterface or standalone version | |
| Suspicious Indicators | 14 |



| | |
|---|---|
| Reads the active computer name | ▼ |
| Reads the cryptographic machine GUID | ▼ |
| Tries to sleep for a long time (more than two minutes) | ▼ |
| External Systems | |
| Found an IP/URL artifact that was identified as malicious by at least one reputation engine | ▼ |
| General | |
| Requested access to a system service | ▼ |
| Sent a control code to a service | ▼ |
| Installation/Persistence | |
| Drops executable files | ▼ |
| Modifies auto-execute functionality by setting/creating a value in the registry | ▼ |
| Spyware/Information Retrieval | |
| Contains ability to retrieve keyboard strokes | ▼ |
| System Security | |
| Modifies proxy settings | ▼ |
| Queries sensitive IE security settings | ▼ |
| Unusual Characteristics | |
| Installs hooks/patches the running process | ▼ |
| Reads information about supported languages | ▼ |
| Hiding 1 Suspicious Indicators | |



Informative

12

Environment Awareness

Reads the registry for installed applications

General

An application crash occurred

Contacts domains

Contacts server

Creates a writable file in a temporary directory

Creates mutants

Loads the .NET runtime environment

Spawns new processes

Installation/Persistence

Dropped files

Touches files in the Windows directory

Network Related

Found potential URL in binary/memory

Unusual Characteristics


Matched Compiler/Packer signature

File Details


All Details: ☐ Off

HYBRID
ANALYSIS

■ taskmgr.exe

| | |
|-----------------|--|
| Filename | taskmgr.exe |
| Size | 24KiB (24064 bytes) |
| Type | peexeassemblyexecutable |
| Description | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Architecture | WINDOWS |
| SHA256 | 07e789f4f2f3259e7559fdccb36e96814c2dbff872a21e1fa03de9ee377d581f  |
| Compiler/Packer | Microsoft visual C# v7.0 / Basic .NET |
| PDB Pathway | |

Resources

| | |
|----------|---|
| Language | NEUTRAL |
| Icon |  |

Visualization

Input File (PortEx)



Classification (TrID)

- 55.8% (.EXE) Generic CIL Executable (.NET, Mono, etc.)
- 21.0% (.EXE) Win64 Executable (generic)
- 9.9% (.SCR) Windows Screen Saver
- 5.0% (.DLL) Win32 Dynamic Link Library (generic)
- 3.4% (.EXE) Win32 Executable (generic)

File Sections

Details

| | |
|-----------------|----------------------------------|
| Name | .text |
| Entropy | 5.57071994207 |
| Virtual Address | 0x2000 |
| Virtual Size | 0x5494 |
| Raw Size | 0x5600 |
| MD5 | f7515b541984adee280ba8b354a0ef1d |

| | |
|------|-------|
| Name | .rsrc |
|------|-------|



Virtual Size 0x240
Raw Size 0x400
MD5 0243c9a7f8755f2c2b18037cdad6cc91

Name .reloc
Entropy 0.0815394123432
Virtual Address 0xa000
Virtual Size 0xc
Raw Size 0x200
MD5 8f9fb76ec87ec8b0a5110a8a33506bf3

File Resources

Details

Name RT_MANIFEST
RVA 0x8058
Size 0x1e7
Type XML 1.0 document, ASCII text, with CRLF line terminators
Language Neutral

File Imports

mscoree.dll

_CorExeMain

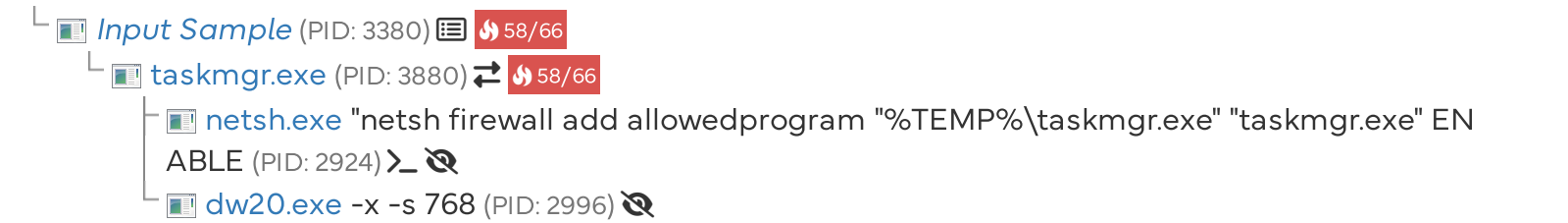
Screenshots

Loading content, please wait...

Hybrid Analysis



Analysed 4 processes in total.



| | | | |
|---------------------|------------------|-------------------|-----------------|
| 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 |
|--------------------------|--------------|---|---------|
| youssefelmi.ddns.net | 197.0.152.18 | TLDS LLC. d/b/a SRSPPlus Organization: No-IP.com Name Server: NF1.NO-IP.COM Creation Date: Thu, 28 Jun 2001 00:00:00 GMT | Tunisia |

Contacted Hosts

Login to Download Contacted Hosts (CSV)

| IP Address | Port/Protocol | Associated Process | Details |
|--------------|---------------|--------------------------|---------|
| 197.0.152.18 | 1177 TCP | taskmgr.exe PID: 3880 | Tunisia |

Contacted Countries



HTTP Traffic

No relevant HTTP requests were made.

Memory Forensics

| String | Context | Stream UID |
|----------------------|---------------------|--|
| youssefelmi.ddns.net | Domain/IP reference | 1513b3984eeafa346728799966dd4728-6000001-cctor |

Extracted Strings

Q

Search

All Details:

Off

Download All Memory Strings (1.3KiB)

All Strings (255)

Interesting (134)

07e789f4f2f3259e7559fd...

taskmgr.exe:3880 (1)

netsh.exe (1)

dw20.exe (1)

taskmgr.exe.2789317516 (18)

screen_0.png (1)

07e789f4f2f3259e7559fd...

netsh.exe:2924 (10)

network.pcap (2)

"%TEMP%\taskmgr.exe" ..

[ENTER]\r\n

[TAP]\r\n

Malicious

1

taskmgr.exe

[👤 Overview](#)
[⬇️ Download Disabled](#)
[👁 Extended File Details](#)
[📄 VirusTotal Report](#)
[🔍 Looking for file context ...](#)

Size 24KiB (24064 bytes)

Type **peexe** **assembly** **executable**

| | |
|--------------------|--|
| Description | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
|--------------------|--|

AV Scan Result Labeled as "Generic.MSIL.Bladabindi" (58/66)

Runtime Process dw20.exe (PID: 2996)

MD5 1513b3984eeafa346728799966dd4728 

SHA1 a0231d04ae17e9a400b32e2b06353e654df3418c

SHA256 07e789f4f2f3259e7559fdccb36e96814c2dbff872a21e1fa03de9ee377d581f 



Community

! There are no community comments.

! You must be logged in to submit a comment.