

taskmgr.exe 🔗

malicious

This report is generated from a file or URL submitted to this webservice on October 9th 2017 20:10:46 Threat Score: 100/100 (UTC) and action script *Heavy Anti-Evasion* AV Detection: 93%
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by [Falcon Sandbox](#) © Hybrid Analysis

Labeled as: [Trojan.Generic](#)

#njrati

#rati

🔗 Overview

🔒 Sample unavailable

📄 Downloads

📄 External Reports

✕ Post

🔗 Link

📧 E-Mail

🔄 Re-analyze

🔒 Hash Not Seen Before

🔗 Show Similar Samples

📄 Report False-Positive

⚠️ Request Report Deletion

Incident Response

👁 Risk Assessment

Remote Access	Uses network protocols on unusual ports
Persistence	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
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID
Evasive	Tries to sleep for a long time (more than two minutes)
Network Behavior	Contacts 1 domain and 1 host. 🔍 View all details

Incident Response

Indicators

- Malicious (10)
- Suspicious (14)
- Informative (12)

File Details

Screenshots (1)

Hybrid Analysis (4)

Network Analysis

Extracted Strings

Extracted Files (1)

Notifications

Community (0)

[Back to top](#)

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

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

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

HYBRID ANALYSIS

Request Info

Q


×

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

 taskmgr.exe

Filename

taskmgr.exe

Size

24KiB (24064 bytes)

Type

peexe

assembly

executable

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

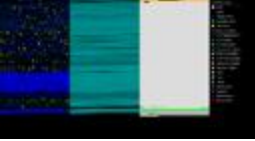
NEUTRAL

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)

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 3 of 6

.text	5.57071994207	0x2000	0x5494	0x5600	f7515b541984adee280ba8b354a0ef1d	-
.rsrc	4.9660813397	0x8000	0x240	0x400	0243c9a7f8755f2c2b18037cdad6cc91	-
.reloc	0.0815394123432	0xa000	0xc	0x200	8f9fb76ec87ec8b0a5110a8a33506bf3	-

File Resources

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


File Imports

mscoree.dll
_CorExeMain

Screenshots

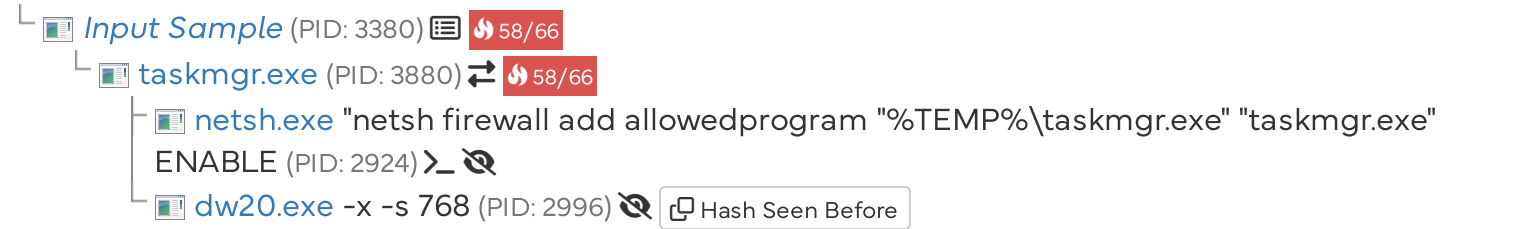


Hybrid Analysis



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

Analysed 4 processes in total.



Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activityy	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	Tunisia

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](#)

Extracted Files

Malicious1

 taskmgr.exe

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Not Seen Before

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 

Notifications

Runtime

Community

 There are no community comments.

 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](#)