

JoeSandbox Cloud BASIC



ID: 433018

Sample Name: icudt63.dll.txt

Cookbook: default.jbs

Time: 06:20:16

Date: 11/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report icudt63.dll.txt	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
General Information	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	7
Static PE Info	8
General	8
Authenticode Signature	8
Entrypoint Preview	8
Data Directories	8
Sections	8
Resources	8
Exports	8
Version Infos	8
Network Behavior	8
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: notepad.exe PID: 5608 Parent PID: 5692	9
General	9
File Activities	9
Disassembly	9
Code Analysis	9

Analysis Report icudt63.dll.txt

Overview

General Information

Sample Name:

icudt63.dll.txt

Analysis ID:

433018

MD5:

7307885d1b4d6e..

SHA1:

9ccb3a49ab72e7..

SHA256:

bb79555ab9fe209.

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

2

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

PE / OLE file has an invalid certificate

PE file contains an invalid checksum

PE file does not import any functions

Queries the volume information (nam...

Uses 32bit PE files

Classification

Process Tree

- System is w10x64
- notepad.exe (PID: 5608 cmdline: 'C:\Windows\system32\notepad.exe' C:\Users\user\Desktop\icudt63.dll.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

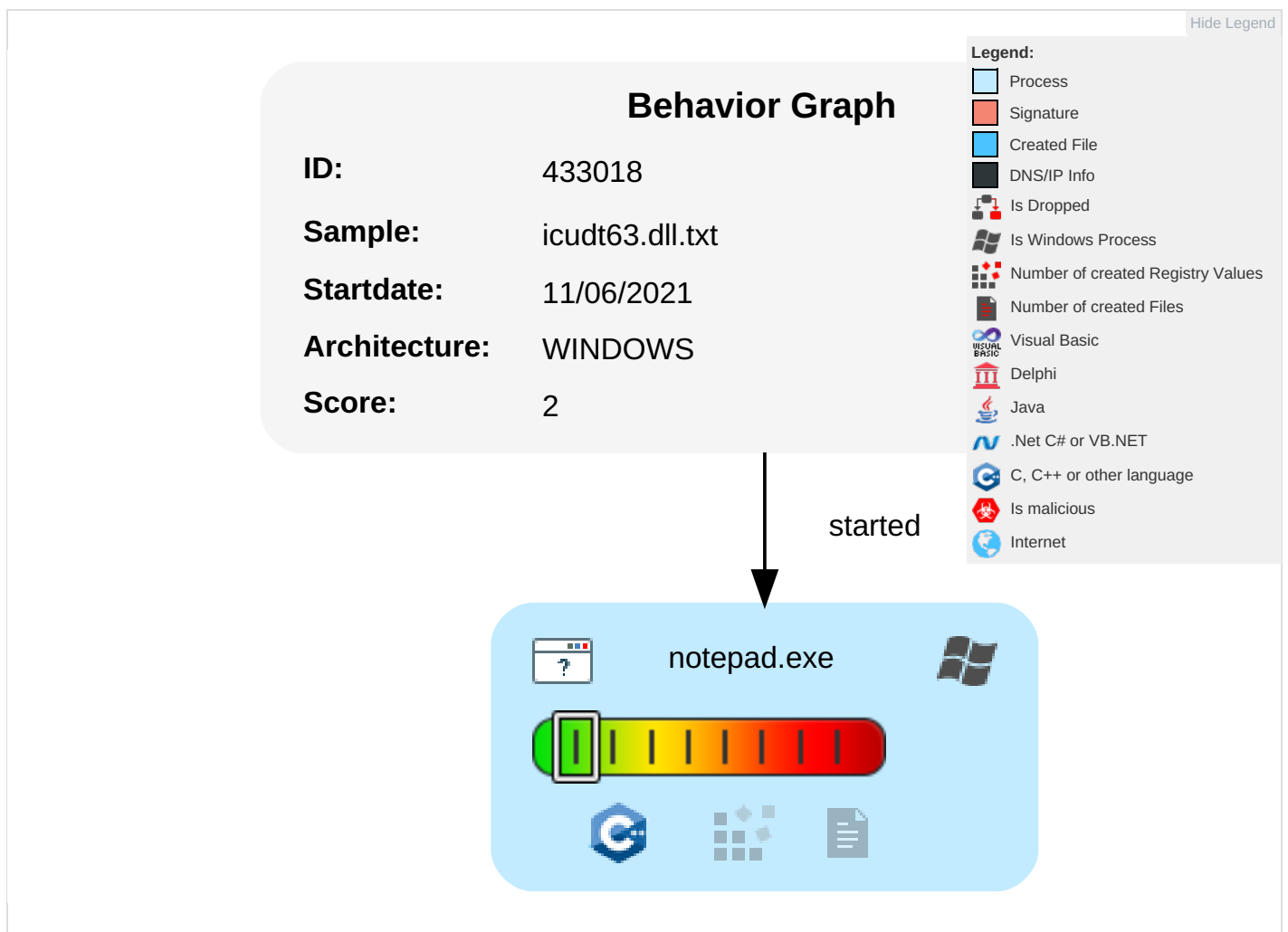
Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Behavior Graph

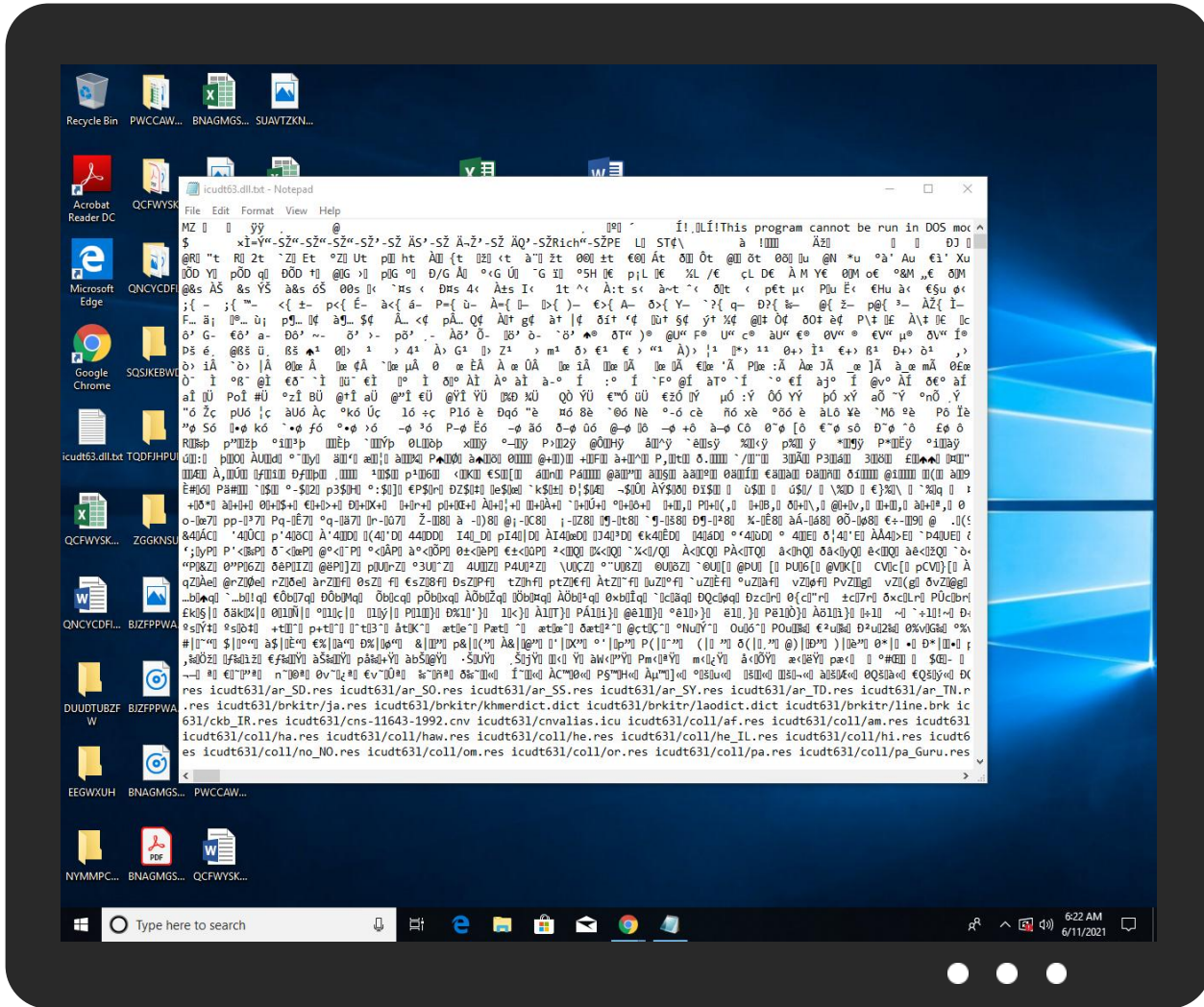
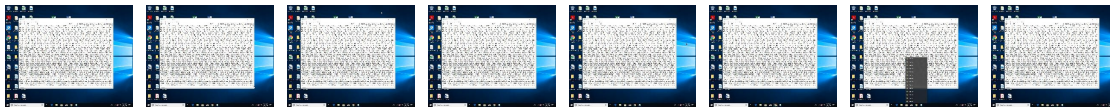


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
icudt63.dll.txt	2%	Virusotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433018
Start date:	11.06.2021
Start time:	06:20:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	icudt63.dll.txt
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.winTXT@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .txt
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context


Created / dropped Files

No created / dropped files found

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.214477136647996
TrID:	<ul style="list-style-type: none">Win32 Dynamic Link Library (generic) (1002004/3) 99.60%Generic Win/DOS Executable (2004/3) 0.20%DOS Executable Generic (2002/1) 0.20%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	icudt63.dll.txt
File size:	27192000
MD5:	7307885d1b4d6e86c16cd3245149a2b5
SHA1:	9ccb3a49ab72e765088aaa78648eaad54e859f25
SHA256:	bb79555ab9fe2098b6d2ddb5b871558303e87a4bdf652cbad66100dfa52d431
SHA512:	2f53fb198e902b01d500c560a09f6dd5eecacfd1208b84721741bc7b442b3016a591086c15660cfd5b05a973041b51f6db07be79e31201a99786cea0dc8067fd
SSDEEP:	393216:7LAzFAVexVyB3uFidiXUxempfJclWlj3qUI2n1g9WbknRy2DS/auO47Tt9r0PohFa:weVexVV9
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......=...S... S...S...S...S...S.....S...Q...S.Rich..S.PE..L...ST.\..... ...!.....J.....

File Icon

	
Icon Hash:	74f4e4e4e4e4e4e4

Static PE Info

General

Entrypoint:	0x4ad00000
Entrypoint Section:	
Digitally signed:	true
Imagebase:	0x4ad00000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	NO_SEH, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5CA25453 [Mon Apr 1 18:11:31 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	

Authenticode Signature

Signature Valid:	false
Signature Issuer:	CN=COMODO RSA Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	The digital signature of the object did not verify
Error Number:	-2146869232
Not Before, Not After	<ul style="list-style-type: none">3/16/2016 5:00:00 PM 3/17/2021 4:59:59 PM
Subject Chain	<ul style="list-style-type: none">CN=Open Text Corporation, OU=Development, O=Open Text Corporation, STREET=275 Frank Tompa, L=Waterloo, S=Ontario, PostalCode=N2L0A1, C=CA
Version:	3
Thumbprint MD5:	1CBB24700ACBA67F3C3BC1267F75960F
Thumbprint SHA-1:	B9443AE8AB96FEC5B7DCE3D22AB6B0A6309F9AF6
Thumbprint SHA-256:	A5F37E0A425E7469FF897C55D5F98E5EB6ABEB3FC834BA27CC0826B5E27E20EA
Serial:	00B8B1587C32F6AB449AC4AFF13F7DBB95

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x19ebc10	0x19ebe00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x19ed000	0x480	0x600	False	0.333333333333	data	2.65267607652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Exports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 5608 Parent PID: 5692

General

Start time:	06:21:02
Start date:	11/06/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\notepad.exe' C:\Users\user\Desktop\icudt63.dll.txt
Imagebase:	0x7ff7977d0000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis