

JOeSandbox Cloud BASIC



ID: 500395

Sample Name: 650912 .xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 00:21:11

Date: 12/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report 650912 .xls	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	3
E-Banking Fraud:	4
System Summary:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
General Information	6
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static OLE Info	8
General	8
OLE File "650912 .xls"	9
Indicators	9
Summary	9
Document Summary	9
Streams with VBA	9
Streams	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: EXCEL.EXE PID: 6892 Parent PID: 800	9
General	9
File Activities	10
File Created	10
Registry Activities	10
Key Created	10
Key Value Created	10
Disassembly	10

Windows Analysis Report 650912 .xls

Overview

General Information

Sample Name:	650912 .xls
Analysis ID:	500395
MD5:	5b239ac2b45218...
SHA1:	abefd9905f25fdc...
SHA256:	f3ff9603b23796a...
Tags:	bft Gozi isfb ursnif xls
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

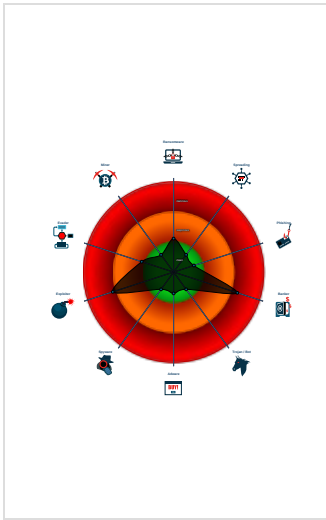
Ursnif Dropper

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Detected Italy targeted Ursnif droppe...
- Document contains an embedded VB...
- Document contains embedded VBA ...

Classification



Process Tree

- System is w10x64
- EXCEL.EXE (PID: 6892 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

E-Banking Fraud:



Detected Italy targeted Ursnif dropper document

System Summary:

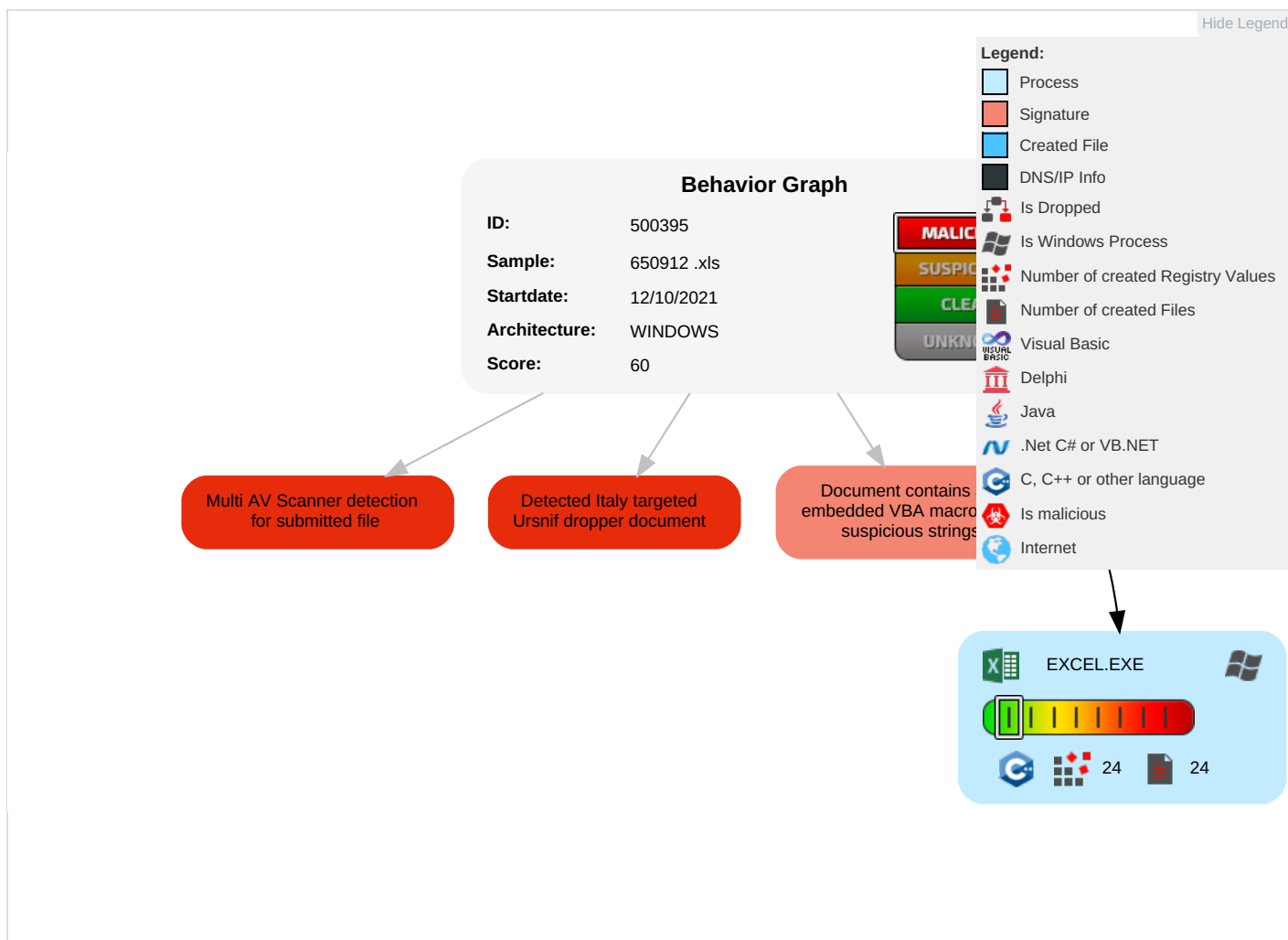


Document contains an embedded VBA macro with suspicious strings

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	Scripting 1 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory 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	Scripting 1 1	LSASS Memory	System Information Discovery 2	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

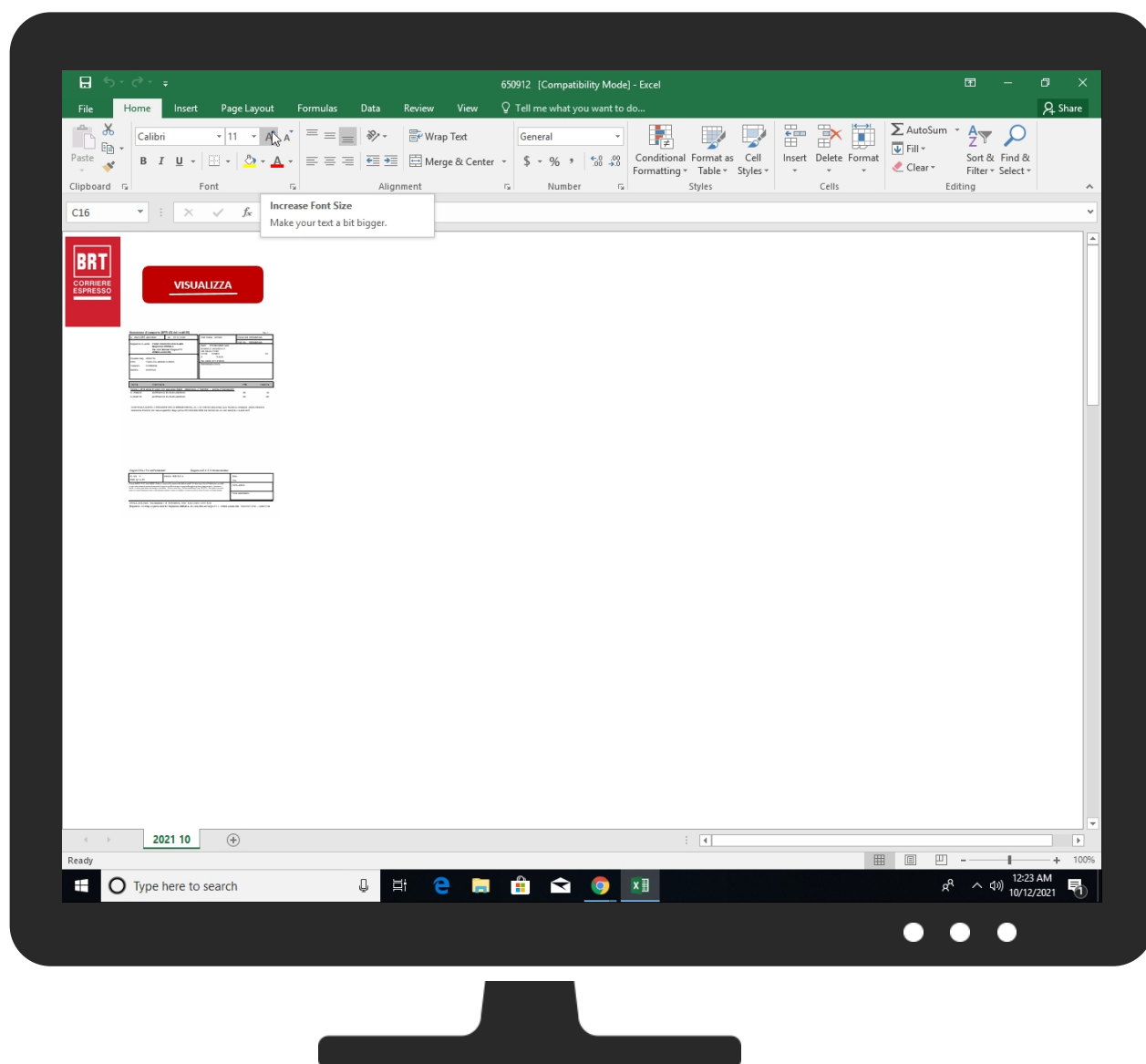
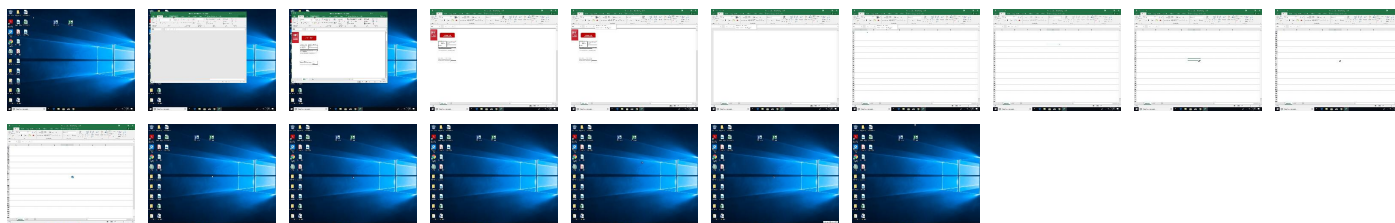
Behavior Graph



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
650912 .xls	17%	Virustotal		Browse
650912 .xls	20%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

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:	33.0.0 White Diamond
Analysis ID:	500395

Start date:	12.10.2021
Start time:	00:21:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	650912 .xls
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	15
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.bank.expl.winXLS@1/1@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active Picture Object • Active AutoShape Object • Scroll down • Close Viewer
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

C:\Users\user1\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\35F6661B-AEDB-44E3-949D-A83F70583589	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	138049
Entropy (8bit):	5.35939982820714
Encrypted:	false
SSDEEP:	1536:WcQIKNZrBdA3gBwfnQ9DQW+zBY34Zzi7nXboOidXVE6LWME9:iWQ9DQW+zbXa1
MD5:	B999163D9F5ED147B2EE7950DBD3C0D4
SHA1:	0059385F2E773D1046E89AF4BAED49FC275341D1
SHA-256:	D1CE71F6E0E13E91F64E7D2B147BA4E9D1FDEE48BDE2B7FE1CC4FD73B73A21F7
SHA-512:	4BAA051313D905231F5A4E1CB901E6D6CD07868AA8091D45C9B79A82A523D71F2DE7A609B0BD00DCCEE6D5D17C035DE25EFF18B9797A4196C3A71352B37690A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">..<o:services o:GenerationTime="2021-10-11T22:22:13">..Build: 16.0.14604.30525-->..<o:default>..<o:ticket o:headerName="Authorization" o:headerValue="{}" />..</o:default>..<o:service o:name="Research">..<o:url>https://rr.office.microsoft.com/research/query.aspx</o:url>..</o:service>..<o:service o:name="ORedir">..<o:url>https://o15.officeredir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="ORedirSSL">..<o:url>https://o15.officeredir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="CIViewClientHelpId">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientHome">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientTemplate">..<o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>..</o:service>..<o:

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Create Time/Date: Mon Oct 11 09:03:47 2021, Last Saved Time/Date: Mon Oct 11 09:03:49 2021, Security: 0, Comments: "BRT"
Entropy (8bit):	5.314831852450583
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	650912 .xls
File size:	51712
MD5:	5b239ac2b45218ad505553d52203c744
SHA1:	abefd9905f25fdcea76783cfd877c19206d117ab
SHA256:	f3ff9603b23796a30d10ae2cfa0001212752705a3e602371ae74d0f4d8defb71
SHA512:	af1bb5477e46cc4ed1177a0b48a6d187b2a45fa68a28291f10466d85816bae8d6ba1ad1579f1b1f6ef4d276ad73efd98cebf4fe7071349769c6a93dc0cbda5fd
SSDEEP:	1536:dsQIYkElbSkKBEqEXPGsRZmbaoFhZhR0cixIHm0THPFDI0LF/yUKAmsiwc:dhLYkEluPm3fNRRZmbaoFhZhR0cixIHmP
File Content Preview:	>.....:.....

File Icon

	
Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
----------------	-----

General

Number of OLE Files:	1
----------------------	---

OLE File "650912 .xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Comments:	"BRT
Create Time:	2021-10-11 08:03:47.102000
Last Saved Time:	2021-10-11 08:03:49
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6892 Parent PID: 800

General

Start time:	00:22:12
-------------	----------

Start date:	12/10/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x80000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

[File Activities](#)

Show Windows behavior

File Created

[Registry Activities](#)

Show Windows behavior

Key Created

Key Value Created

Disassembly