ID: 800705
Sample Name: readme.txt
Cookbook: default.jbs
Time: 18:27:05
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

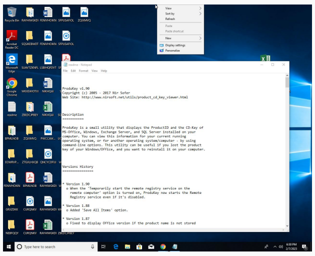
Windows Analysis Report

readme.txt

Overview

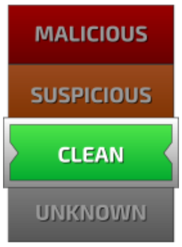
General Information

Sample Name:	readme.txt
Analysis ID:	800705
MD5:	99a47df2646f1…
SHA1:	a32553c3ad3a…
SHA256:	a7e78fdcad18f…



```
ProduKey v1.90
Copyright (c) 2005 - 2017 Nir Sofer
Web Site: http://www.nirsoft.net/utils/product_cd_key_viewer.html



Description
===========

ProduKey is a small utility that displays the ProductID and the CD-Key of
MS-Office, Windows, Exchange Server, and SQL Server installed on your
computer. You can view this information for your current running
operating system, or for another operating system/computer - by using
command-line options. This utility can be useful if you lost the product
key of your Windows/Office, and you want to reinstall it on your computer.



Versions History
================


* Version 1.90
  o When the 'Temporarily start the remote registry service on the
    remote computer' option is turned on, ProduKey now starts the Remote
    Registry service even if it's disabled.

* Version 1.88
  o Added 'Save All Items' option.

* Version 1.87
  o Fixed to display Office version if the product name is not stored
```

Detection

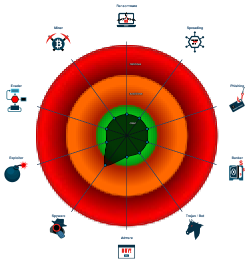


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- notepad.exe (PID: 5200 cmdline: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\readme.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

⊘ **No configs have been found**

Yara Signatures

⊘ **No yara matches**

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

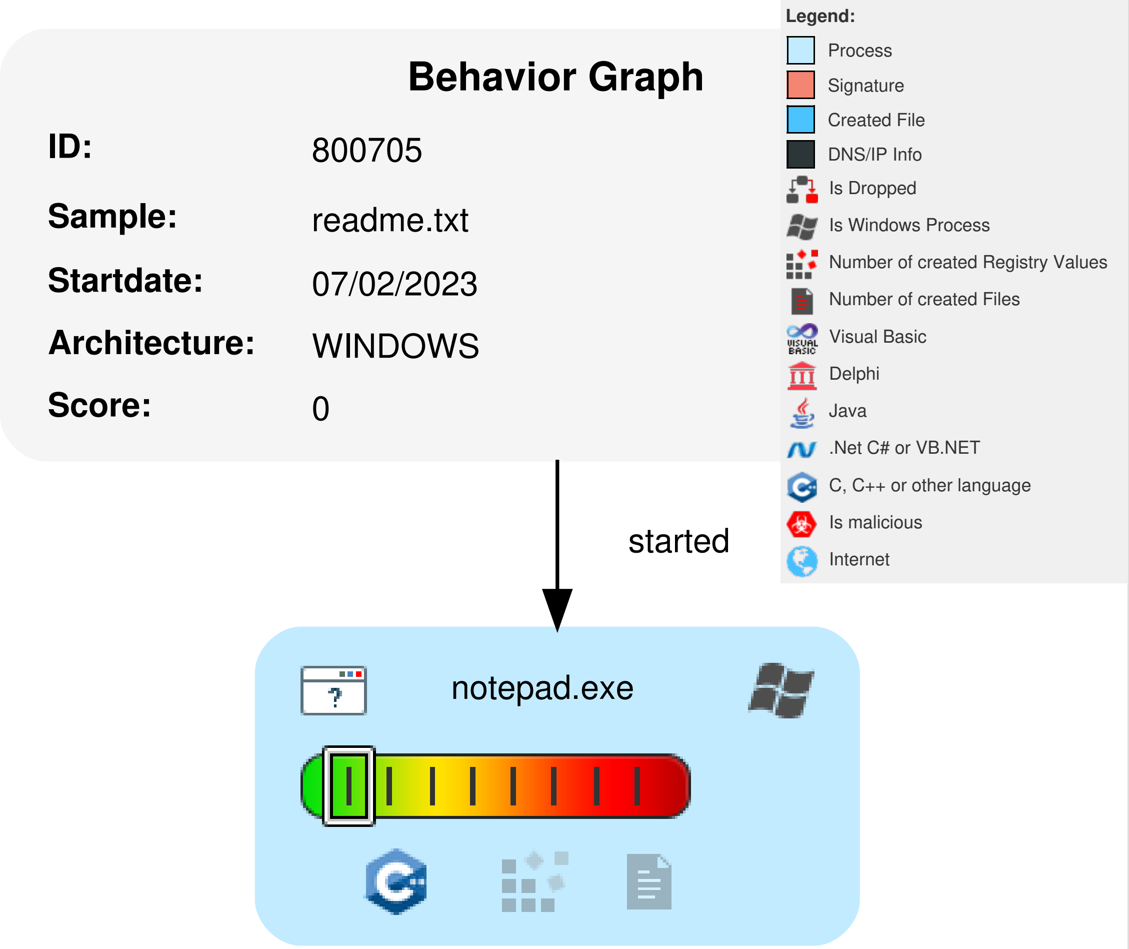
There are no malicious signatures, click here to show all signatures.

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	Path Interception	Direct Volume Access	OS Credential Dumping	1 1 System Information Discovery	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

Behavior Graph

Hide Legend



Behavior Graph

ID: 800705

Sample: readme.txt

Startdate: 07/02/2023

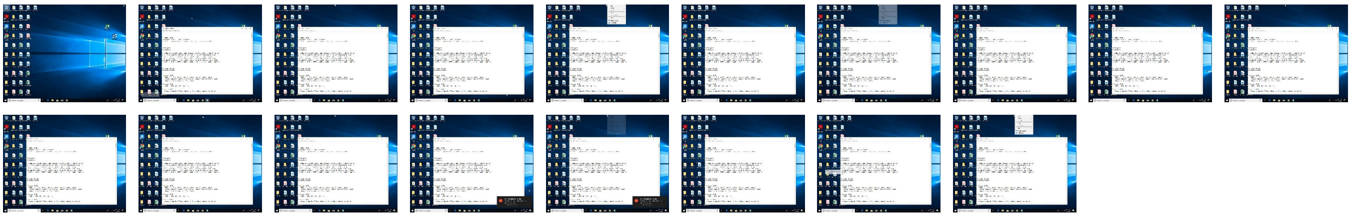
Architecture: WINDOWS

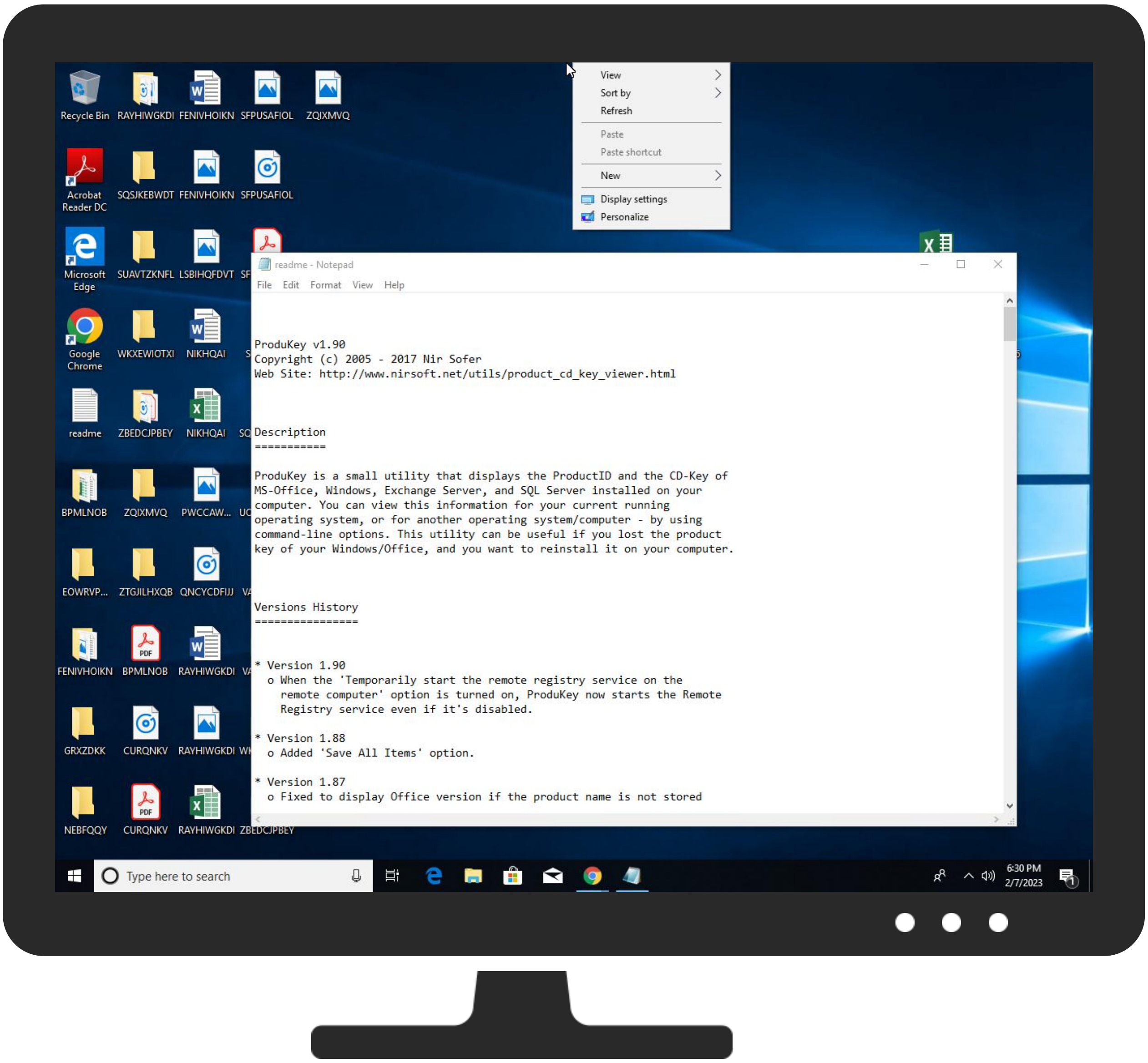
Score: 0

Screenshots

Thumbnails

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





```
ProduKey v1.90
Copyright (c) 2005 - 2017 Nir Sofer
Web Site: http://www.nirsoft.net/utils/product_cd_key_viewer.html



Description
===========

ProduKey is a small utility that displays the ProductID and the CD-Key of
MS-Office, Windows, Exchange Server, and SQL Server installed on your
computer. You can view this information for your current running
operating system, or for another operating system/computer - by using
command-line options. This utility can be useful if you lost the product
key of your Windows/Office, and you want to reinstall it on your computer.



Versions History
================


* Version 1.90
  o When the 'Temporarily start the remote registry service on the
    remote computer' option is turned on, ProduKey now starts the Remote
    Registry service even if it's disabled.

* Version 1.88
  o Added 'Save All Items' option.

* Version 1.87
  o Fixed to display Office version if the product name is not stored
```

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
readme.txt	0%	ReversingLabs		
readme.txt	0%	Virustotal		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

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/utils/product_cd_key_viewer.html	notepad.exe, 00000000.00000002.575681616.0000021BE0599000.00000004.00000020.00020000.00000000.sdmp, readme.txt	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800705
Start date and time:	2023-02-07 18:27:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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
Sample file name:	readme.txt
Detection:	CLEAN
Classification:	clean0.winTXT@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .txt

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

⊘ **No simulations**

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

⊘ **No created / dropped files found**

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	4.897628741856098
TrID:	
File name:	readme.txt
File size:	17399
MD5:	99a47df2646f18b7f94f1d29c236c93a

SHA1:	a32553c3ad3abe7fe4431aea637c82539d9d8d3f
SHA256:	a7e78fdcad18f8f3be24d4fa4aee23cbf1a138497479469e4e1ad79640330add
SHA512:	e58dc4a5592eb9f80c6d9580d047b34e0e08e257896e4c28afccaca3e14457c3a611e7813928cd3f6ad159f9c204ada1b0126b917cdafb1c60aa6093589d22fc
SSDEEP:	192:WmsnCqMzjGrGkgbbxgZ7eQ6POTTenmfOUj0ySRLSHFYHOf7WL8K6pt9WDaIGec2X:WuqGaeQ6PGTFvjv8Sl0AIG6ewt4NsAS
TLSH:	1A72564BD1AB133211B302A356CD7BC3FB6941699786892474ADD31C2327B4AE3BB4DD
File Content Preview:	......ProduKey v1.90..Copyright (c) 2005 - 2017 Nir Sofer..Web Site: http://www.nirsoft.net/utils/product_cd_key_viewer.html........Description..===========....ProduKey is a small utility that displays the ProductID and the CD-Key of..MS-Office, Windows,

File Icon

Icon Hash:	74f4e4e4e4e4e4e4

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

⊘ **No statistics**

System Behavior

Analysis Process: notepad.exe PID: **5200**, Parent PID: **3324**

General

Target ID:	0
Start time:	18:28:04
Start date:	07/02/2023
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\readme.txt
Imagebase:	0x7ff6b07c0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

⊘ **No disassembly**