ID: 635353
Sample Name: MD5 & SHA Checksum Utility.exe
Cookbook: default.jbs
Time: 20:03:39
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

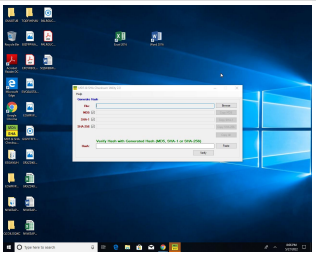
Windows Analysis Report

MD5 & SHA Checksum Utility.exe

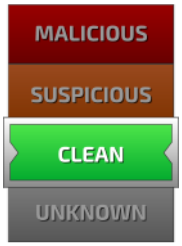
Overview

General Information

Sample Name:	MD5 & SHA Checksum Utility.exe
Analysis ID:	635353
MD5:	88a40aa4a04f93..
SHA1:	e0182fde50ebfbe.
SHA256:	1dcbf036ef010c3..
Infos:	



Detection

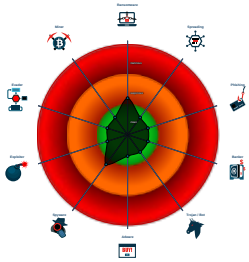


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- Program does not show much activi…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- MD5 & SHA Checksum Utility.exe (PID: 6448 cmdline: "C:\Users\user\Desktop\MD5 & SHA Checksum Utility.exe" MD5: 88A40AA4A04F9391336E7DB258A3B16C)
- **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

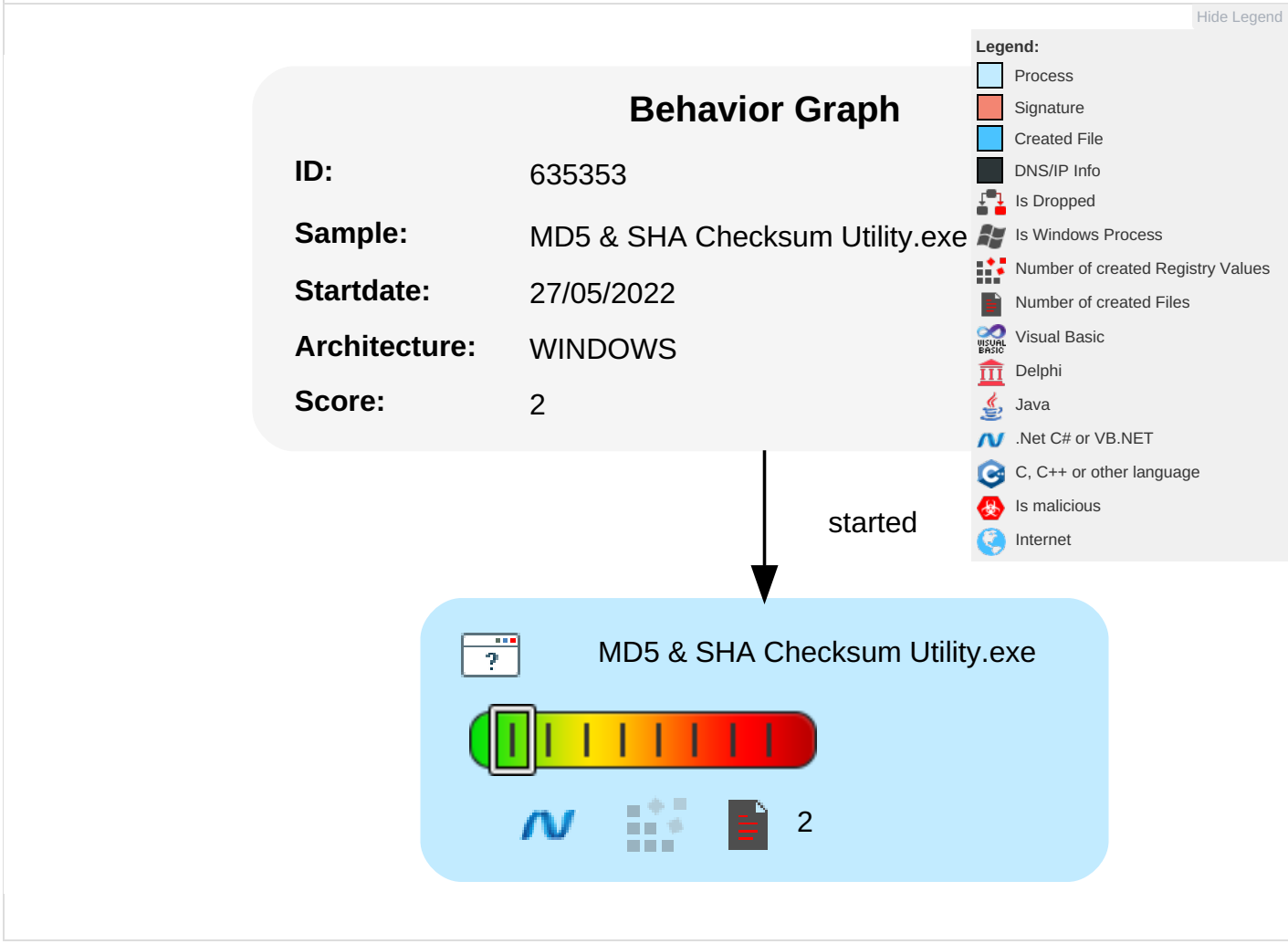
Joe Sandbox Signatures

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	1 Disable or Modify Tools	OS Credential Dumping	1 1 System Information Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

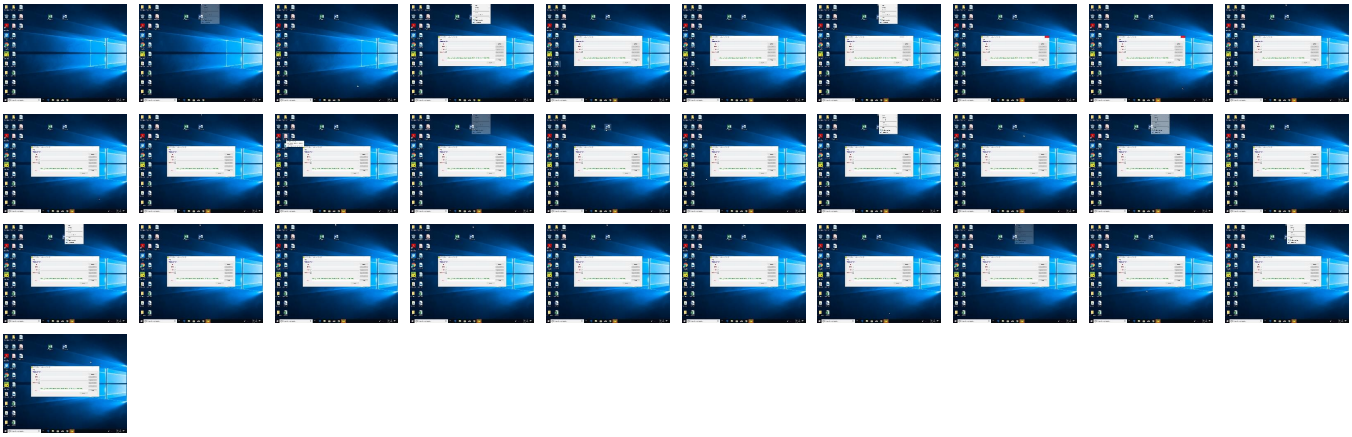
Behavior Graph

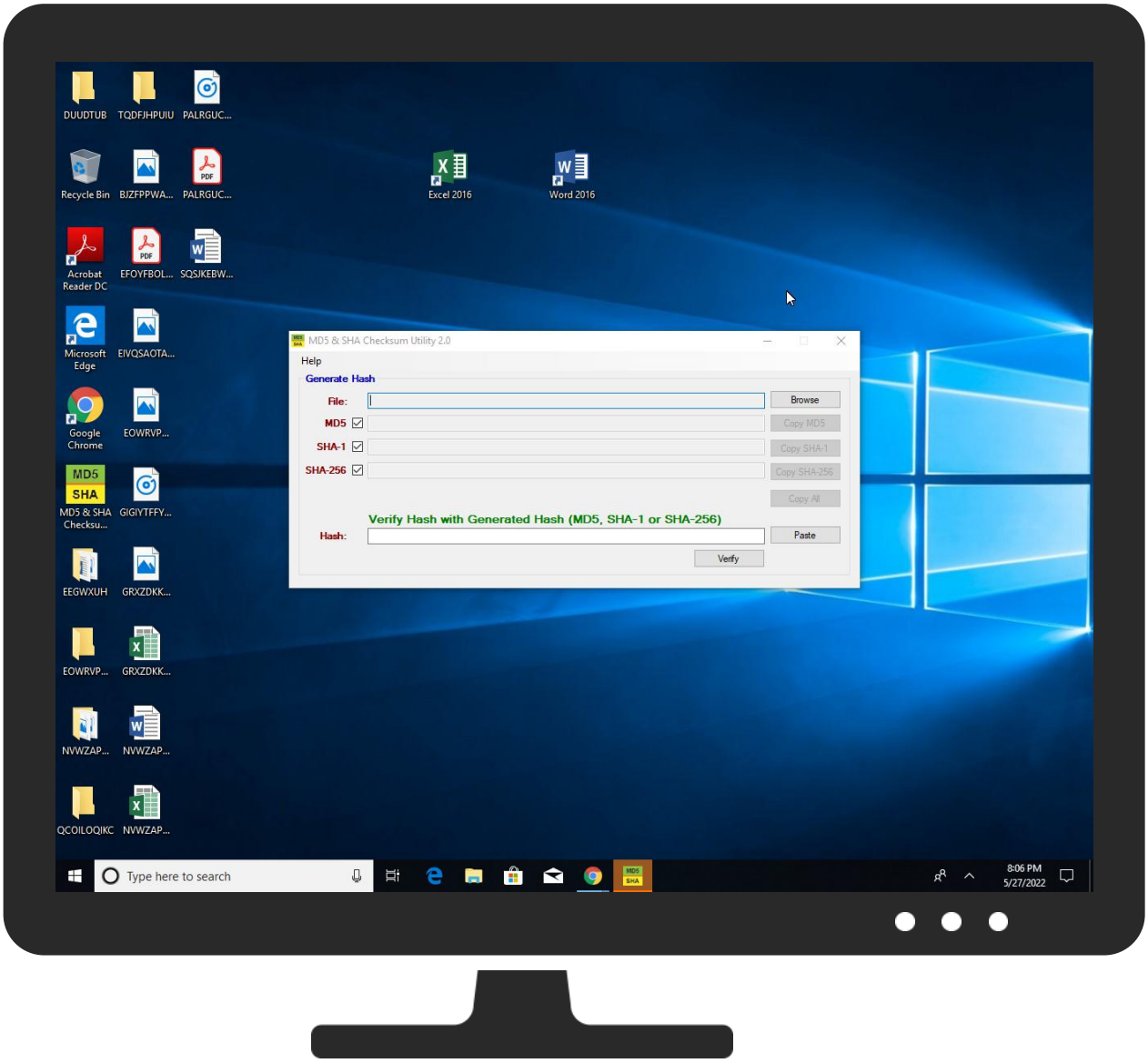


Screenshots

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
MD5 & SHA Checksum Utility.exe	3%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
MD5 & SHA Checksum Utility.exe	0%	Metadefender		Browse
MD5 & SHA Checksum Utility.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0TC	0%	Virustotal		Browse
http://www.jiyu-kobo.co.jp/Y0TC	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comar	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com(N	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com_2(	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sakkal.comn	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comD	0%	URL Reputation	safe	
http://www.fontbureau.comva	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/a%	0%	Avira URL Cloud	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/h	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//F	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn.cn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comH	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.sajatypeworks.comL2	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.sajatypeworks.comlar	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a%	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kral	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krim	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.fontbureau.comx	0%	URL Reputation	safe	
http://www.founder.com.cn/cnom	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0TC	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comar	MD5 & SHA Checksum Utility.exe, 00000000.00000003.267404201.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com(N	MD5 & SHA Checksum Utility.exe, 00000000.00000003.267397562.000000001C157000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com_2(	MD5 & SHA Checksum Utility.exe, 00000000.00000003.267397562.000000001C157000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility	MD5 & SHA Checksum Utility.exe	false		high
http://www.tiro.com	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275337462.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	MD5 & SHA Checksum Utility.exe, 00000000.00000003.272194950.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272379429.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272478884.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272286427.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersP	MD5 & SHA Checksum Utility.exe, 00000000.00000003.278233734.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278180953.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.267404201.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.267397562.000000001C157000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://raylin.wordpress.com	MD5 & SHA Checksum Utility.exe	false		high
http://www.sakkal.comn	MD5 & SHA Checksum Utility.exe, 00000000.00000003.274077247.000000001C154000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comD	MD5 & SHA Checksum Utility.exe, 00000000.00000003.272379429.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272286427.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comva	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275149311.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnm	MD5 & SHA Checksum Utility.exe, 00000000.00000003.270774497.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.270678522.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.270613242.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/a%	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273680651.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.net	MD5 & SHA Checksum Utility.exe, 00000000.00000003.268338463.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/h	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://raylin.wordpress.com/donate/	MD5 & SHA Checksum Utility.exe	false		high
http://www.galapagosdesign.com/DPlease	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//F	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273369750.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273621567.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	MD5 & SHA Checksum Utility.exe, 00000000.00000003.274077247.000000001C154000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersoi	MD5 & SHA Checksum Utility.exe, 00000000.00000003.278233734.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278180953.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.269906441.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273989910.000000001C15D000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersiv	MD5 & SHA Checksum Utility.exe, 00000000.00000002.526737986.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278233734.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.279463796.000000001C169000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278180953.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275250508.000000001C158000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.276324149.000000001C15D000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275353411.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275640604.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275149311.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278180953.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.276139153.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275988193.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275369939.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn.cn	MD5 & SHA Checksum Utility.exe, 00000000.00000003.272038725.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275674496.000000001C157000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comH	MD5 & SHA Checksum Utility.exe, 00000000.00000003.276324149.000000001C15D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/P	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comL2	MD5 & SHA Checksum Utility.exe, 00000000.00000003.267397562.000000001C157000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krh	MD5 & SHA Checksum Utility.exe, 00000000.00000003.269906441.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/F	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273464161.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273485035.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273369750.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comlar	MD5 & SHA Checksum Utility.exe, 00000000.00000003.267404201.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comlic	MD5 & SHA Checksum Utility.exe, 00000000.00000003.278233734.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.278180953.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273464161.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273485035.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273515915.000000001C169000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273621567.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	MD5 & SHA Checksum Utility.exe, 00000000.00000003.272777292.000000001C168000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272938164.000000001C169000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.267674688.000000001C154000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.272927142.000000001C169000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a%	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273464161.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273485035.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273515915.000000001C169000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273621567.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273369750.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	MD5 & SHA Checksum Utility.exe, 00000000.00000003.270750257.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.270678522.000000001C16C000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.270613242.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/F/	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273680651.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273621567.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kral	MD5 & SHA Checksum Utility.exe, 00000000.00000003.269688165.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273464161.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273485035.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273515915.000000001C169000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273680651.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273621567.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273840514.000000001C167000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.273369750.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krim	MD5 & SHA Checksum Utility.exe, 00000000.00000003.269688165.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	MD5 & SHA Checksum Utility.exe, 00000000.00000003.272038725.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	MD5 & SHA Checksum Utility.exe, 00000000.00000002.527036030.000000001D362000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/h	MD5 & SHA Checksum Utility.exe, 00000000.00000003.273680651.000000001C16A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comx	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275369939.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	MD5 & SHA Checksum Utility.exe, 00000000.00000003.275149311.000000001C16A000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275369939.000000001C16B000.00000004.00000020.00020000.00000000.sdmp, MD5 & SHA Checksum Utility.exe, 00000000.00000003.275337462.000000001C16B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnom	MD5 & SHA Checksum Utility.exe, 00000000.00000003.270678522.000000001C16C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635353
Start date and time: 27/05/202220:03:39	2022-05-27 20:03:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MD5 & SHA Checksum Utility.exe
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:	23
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:	CLEAN
Classification:	clean2.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target MD5 & SHA Checksum Utility.exe, PID 6448 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory 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:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.652280949045084
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	MD5 & SHA Checksum Utility.exe
File size:	78848
MD5:	88a40aa4a04f9391336e7db258a3b16c
SHA1:	e0182fde50ebfbeab249dd7c4519ffda1fc9e0f5
SHA256:	1dcbf036ef010c301f24bd54cb03ecb15346edefdc0eb3f765aa348422fe5f3b
SHA512:	01d7179a3a71f5c66d0a64eb429b6e5509864734428068e84da3025f848af266d57f6db3c5d26e7dd5d6b1d35080d885fe9199cd21a1432965f1a6e35ccb0fef
SSDEEP:	1536:RiHEOA6Wqswy+GcKY0SQUfmMXUZGW8yQVYS/NoCIFszn42SWRNp5Kk:RiHEOA6Wqswy+GcKY0SQUeMXUZGxyQVX
TLSH:	B173B303EE52D61AD0792EF8017272406EE6A303933DEF893F6DE49A47326405B5AFD5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.Q....."....../... ...@....@.. .....@.....

File Icon

Icon Hash:	2d2727cc93a32348

Static PE Info

General

Entrypoint:	0x412f2e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x51AB61D1 [Sun Jun 2 15:16:33 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12ee0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1f68	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10f34	0x11000	False	0.266745174632	data	5.73085209465	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1f68	0x2000	False	0.198486328125	data	3.5418137372	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x16000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14130	0x1628	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x15758	0x14	data		
RT_VERSION	0x15770	0x320	data		
RT_MANIFEST	0x15a90	0x4d3	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	2.0.0.0
InternalName	MD5 & SHA Checksum Utility.exe
FileVersion	2.0.0.0
ProductName	MD5 & SHA Checksum Utility
ProductVersion	2.0.0.0
FileDescription	MD5 & SHA Checksum Utility
OriginalFilename	MD5 & SHA Checksum Utility.exe

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: MD5 & SHA Checksum Utility.exe PID: **6448**, Parent PID: **1668**

General

Target ID:	0
Start time:	20:04:44
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\MD5 & SHA Checksum Utility.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\MD5 & SHA Checksum Utility.exe"
Imagebase:	0xd20000
File size:	78848 bytes
MD5 hash:	88A40AA4A04F9391336E7DB258A3B16C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60788527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60788527	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC607B5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFC607B5C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC608D5AF3	ReadFile

Disassembly

No disassembly