ID: 1457838
Sample Name:
YY#U6302#U53f7#U534f#U8bae.exe
Cookbook: default.jbs
Time: 20:02:07
Date: 15/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

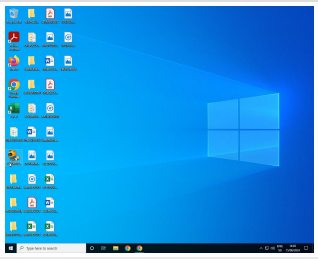
Windows Analysis Report

YY#U6302#U53f7#U534f#U8bae.exe

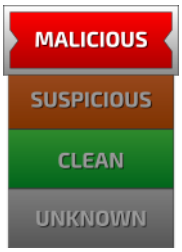
Overview

General Information

Sample name:	YY#U6302#U53f7#U534f#U8bae.exerenamed because original name is a hash value
Original sample name:	YY.exe
Analysis ID:	1457838
MD5:	765cf453d0cea..
SHA1:	060ae0476bbd…
SHA256:	3d76cc27be32…
Tags:	exe
Infos:	



Detection

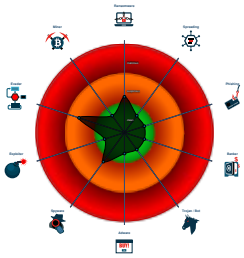


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- AI detected suspicious sample
- Detected VMProtect packer
- Machine Learning detection for sam…
- Contains functionality to check if a d…
- Contains functionality to check the p…
- Contains functionality to dynamicall…
- Contains functionality to query CPU…
- Contains functionality which may be…
- Detected potential crypto function
- Drops PE files
- Drops files with a non-matching file …

Classification



Process Tree

- **System is w10x64**
- YY#U6302#U53f7#U534f#U8bae.exe (PID: 908 cmdline: "C:\Users\user\Desktop\YY#U6302#U53f7#U534f#U8bae.exe" MD5: 765CF453D0CEA3719B619E4C55881093)
- **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

AV Detection

Multi AV Scanner detection for submitted file

AI detected suspicious sample

Machine Learning detection for sample

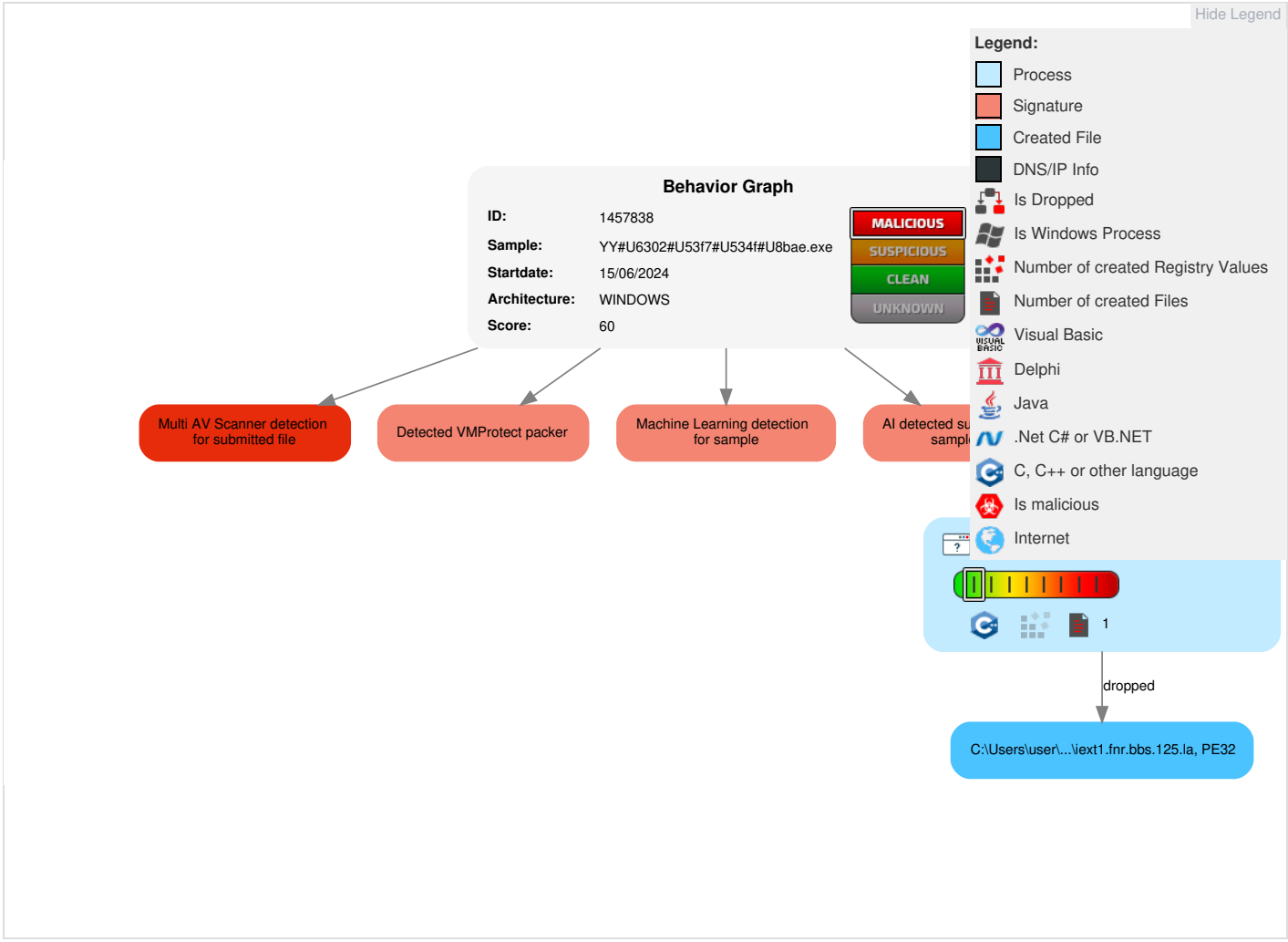
System Summary

Detected VMProtect packer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Native API	1 DLL Side-Loading	1 Process Injection	1 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	3 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	2 Obfuscated Files or Information	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact

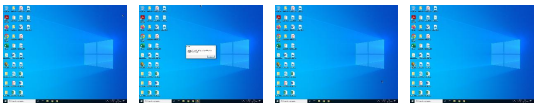
Behavior Graph



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
YY#U6302#U53f7#U534f#U8bae.exe	50%	Virustotal		Browse
YY#U6302#U53f7#U534f#U8bae.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\iext1.fnr.bbs.125.la	5%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.openssl.org/support/faq.html.....rbwb.rndC:HOMERANDFILEPRNG	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://ysapi.yy.com/api/internal/nobleQuery/QueryUserInfoReq.json?data=	0%	Avira URL Cloud	safe	
http://www.yy.com/search-	0%	Avira URL Cloud	safe	
http://https://www.yy.com/zone/assets/total.json	0%	Avira URL Cloud	safe	
http://hgame.yy.com/action/getUserLoginInfo.jsondata.ownChannels	0%	Avira URL Cloud	safe	
http://120.26.95.191:5659/	0%	Avira URL Cloud	safe	
http://www.openssl.org/V	0%	Avira URL Cloud	safe	
http://https://ysapi.yy.com/api/internal/nobleQuery/QueryUserInfoReq.json?data=	0%	Virustotal		Browse
http://https://www.yy.com/zone/assets/total.json	0%	Virustotal		Browse
http://www.yy.com/	0%	Avira URL Cloud	safe	
http://www.openssl.org/V	0%	Virustotal		Browse
http://peipei.yy.com/web/account/internal/account/list	0%	Avira URL Cloud	safe	
http://www.yy.com/	0%	Virustotal		Browse
http://https://www.yy.com/u/	0%	Avira URL Cloud	safe	
http://www.yy.com/search-	0%	Virustotal		Browse
http://bbs.125.la/	0%	Avira URL Cloud	safe	
http://hgame.yy.com/action/getUserLoginInfo.jsondata.ownChannels	NaN%	Virustotal		Browse
http://https://bbs.125.la/thread-14738139-1-1.html	0%	Avira URL Cloud	safe	
http://120.26.95.191:5659/	NaN%	Virustotal		Browse
http://vip.yy.com/service/web/user/info?_time=vipLevel	0%	Avira URL Cloud	safe	
http://https://www.yy.com/u/	0%	Virustotal		Browse
http://www.openssl.org/support/faq.html.....rbwb.rndC:HOMERANDFILEPRNG	0%	Virustotal		Browse
http://peipei.yy.com/web/account/internal/account/list	NaN%	Virustotal		Browse
http://bbs.125.la/	1%	Virustotal		Browse
http://hgame.yy.com/action/getUserLoginInfo.json	0%	Avira URL Cloud	safe	
http://https://www.dmdaili.com/yaoqing/33405.html	0%	Avira URL Cloud	safe	
http://https://captcha.yy.com/baidu/submit.do?appid=	0%	Avira URL Cloud	safe	
http://https://passport.baidu.com/viewlog/getstyle?ak=	0%	Avira URL Cloud	safe	
http://https://bbs.125.la/thread-14738139-1-1.html	1%	Virustotal		Browse
http://vip.yy.com/service/web/user/info?_time=vipLevel	NaN%	Virustotal		Browse
http://https://www.yy.com/zone/userinfo/getUserInfo.json	0%	Avira URL Cloud	safe	
http://https://passport.baidu.com/viewlog/getstyle?ak=	0%	Virustotal		Browse
http://www.openssl.org/support/faq.html	0%	Avira URL Cloud	safe	
http://https://www.dmdaili.com/yaoqing/33405.html	NaN%	Virustotal		Browse
http://https://hd.vip.yy.com/service/hdplatform/drawgift/202402ee1a8f/giftpagingp?drawGiftGroupId=202402ee1	0%	Avira URL Cloud	safe	
http://hgame.yy.com/action/getUserLoginInfo.json	NaN%	Virustotal		Browse
http://https://captcha.yy.com/baidu/submit.do?appid=	0%	Virustotal		Browse
http://https://iexui.com/downexui	0%	Avira URL Cloud	safe	
http://www.openssl.org/support/faq.html	0%	Virustotal		Browse
http://do-dw.yy.com/user.php?sids=	0%	Avira URL Cloud	safe	
http://https://hgame.yy.com/person/p_account	0%	Avira URL Cloud	safe	
http://https://iexui.com/downexui	0%	Virustotal		Browse
http://https://captcha.yy.com/baidu/submit.do?appid=obj	0%	Avira URL Cloud	safe	
http://https://yyfkw.cn	0%	Avira URL Cloud	safe	
http://117.72.34.175:1011/?OrderID=4BA33E0B1BE84295&ipnumber=50	0%	Avira URL Cloud	safe	
http://https://hd.vip.yy.com/service/hdplatform/drawgift/202402ee1a8f/giftpagingp?drawGiftGroupId=202402ee1	NaN%	Virustotal		Browse
http://https://hgame.yy.com/person/p_account	0%	Virustotal		Browse
http://120.26.95.191:5658/	0%	Avira URL Cloud	safe	
http://https://www.yy.com/zone/userinfo/getUserInfo.json	NaN%	Virustotal		Browse
http://https://captcha.yy.com/baidu/submit.do?appid=obj	0%	Virustotal		Browse
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yywebconfigData/giftDatac	0%	Avira URL Cloud	safe	
http://https://yyfkw.cn	0%	Virustotal		Browse
http://vip.yy.com/service/web/user/info?_time=	0%	Avira URL Cloud	safe	
http://120.26.95.191:5658/	NaN%	Virustotal		Browse
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yywebconfigData/giftDatac	0%	Virustotal		Browse
http://vip.yy.com/vip/vcard/indexrest?_time=	0%	Avira URL Cloud	safe	
http://www.yy.com/sid	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.xiequ.cn/index.html?dc1bbee2	0%	Avira URL Cloud	safe	
http://www.uc.cn/ip	0%	Avira URL Cloud	safe	
http://www.yy.com/sid	0%	Virustotal		Browse
http://https://udb.yy.com/authentication.do?action=authenticate&appid=5060&busiUrl=http%3A%2F%2Fwww.yy.com&	0%	Avira URL Cloud	safe	
http://do-dw.yy.com/user.php?sids=	0%	Virustotal		Browse
http://vip.yy.com/service/web/user/info?_time=	0%	Virustotal		Browse
http://https://udb.yy.com/authentication.do?action=authenticate&appid=5060&busiUrl=http%3A%2F%2Fwww.yy.com&	0%	Virustotal		Browse
http://117.72.34.175:1011/?OrderID=4BA33E0B1BE84295&ipnumber=50	NaN%	Virustotal		Browse
http://https://www.yy.com/gu/	0%	Avira URL Cloud	safe	
http://www.uc.cn/ip	0%	Virustotal		Browse
http://www.uc.cn/ipIP:http://	0%	Avira URL Cloud	safe	
http://https://www.yy.com/gu/	0%	Virustotal		Browse
http://https://www.xiequ.cn/index.html?dc1bbee2	NaN%	Virustotal		Browse
http://https://nfnba.lanzoub.com/ietaw0udyhid	0%	Avira URL Cloud	safe	
http://https://yyfkw.cn999https://nfnba.lanzoub.com/ietaw0udyhid	0%	Avira URL Cloud	safe	
http://120.26.95.191:5658/http://120.26.95.191:5659/qq17336171577b2cc005c28c42472000e7863283a212&_=h	0%	Avira URL Cloud	safe	
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yyweb	0%	Avira URL Cloud	safe	
http://https://passport.baidu.com/viewlog?ak=	0%	Avira URL Cloud	safe	
http://https://nfnba.lanzoub.com/ietaw0udyhid	NaN%	Virustotal		Browse
http://vip.yy.com/vip/vcard/indexrest?_time=	0%	Virustotal		Browse
http://channel.yy.com/ajax/member/indexAction	0%	Avira URL Cloud	safe	
http://www.uc.cn/ipIP:http://	0%	Virustotal		Browse
http://120.26.95.191:5658/http://120.26.95.191:5659/qq17336171577b2cc005c28c42472000e7863283a212&_=h	NaN%	Virustotal		Browse
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yyweb	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.openssl.org/support/faq.html.....rbwb.rndC:HOMERANDFILEPRNG	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ysapi.yy.com/api/internal/nobleQuery/QueryUserInfoReq.json?data=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://hgame.yy.com/action/getUserLoginInfo.jsondata.ownChannels	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.yy.com/zone/assets/total.json	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.yy.com/search-	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://120.26.95.191:5659/	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.openssl.org/V	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.yy.com/	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://peipei.yy.com/web/account/internal/account/list	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.yy.com/u/	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://bbs.125.la/	iext1.fnr.bbs.125.la.0.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://bbs.125.la/thread-14738139-1-1.html	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1701213455.0000000002F09000.00000004.00000020.00020000.00000000.sdmp, YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1701495506.000000006CF60000.00000002.00000001.01000000.00000004.sdmp, iext1.fnr.bbs.125.la.0.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://vip.yy.com/service/web/user/info?_time=vipLevel	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://hgame.yy.com/action/getUserLoginInfo.json	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://captcha.yy.com/baidu/submit.do?appid=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.dmdaili.com/yaoqing/33405.html	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://passport.baidu.com/viewlog/getstyle?ak=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.yy.com/zone/userinfo/getUserInfo.json	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.openssl.org/support/faq.html	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://hd.vip.yy.com/service/hdplatform/drawgift/202402ee1a8f/giftpagingp?drawGiftGroupId=202402ee1	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://iexui.com/downexui	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://do-dw.yy.com/user.php?sids=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://hgame.yy.com/person/p_account	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://captcha.yy.com/baidu/submit.do?appid=obj	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://yyfkw.cn	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://117.72.34.175:1011/?OrderID=4BA33E0B1BE84295&ipnumber=50	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000003.1699125254.0000000001351000.00000004.00000020.00020000.00000000.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://120.26.95.191:5658/	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yywebconfigData/giftDatac	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://vip.yy.com/service/web/user/info?_time=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://vip.yy.com/vip/vcard/indexrest?_time=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.yy.com/sid	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.xiequ.cn/index.html?dc1bbee2	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.uc.cn/ip	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://udb.yy.com/authentication.do?action=authenticate&appid=5060&busiUrl=http%3A%2F%2Fwww.yy.com&	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.yy.com/gu/	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.uc.cn/ipIP:http://	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://nfnba.lanzoub.com/ietaw0udyhid	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://yyfkw.cn999https://nfnba.lanzoub.com/ietaw0udyhid	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://120.26.95.191:5658/http://120.26.95.191:5659/qq17336171577b2cc005c28c42472000e7863283a212&_=h	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• NaN%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lxcode.bs2cdn.yy.com/a413808b-e679-47f1-9380-be7b3ebf8813.xml?from=yyweb	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://passport.baidu.com/viewlog?ak=	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://channel.yy.com/ajax/member/indexAction	YY#U6302#U53f7#U534f#U8bae.exe, 00000000.00000002.1699727907.00000000005A0000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1457838
Start date and time:	2024-06-15 20:02:07 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	1
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	YY#U6302#U53f7#U534f#U8bae.exerenamed because original name is a hash value
Original Sample Name:	YY.exe
Detection:	MAL
Classification:	mal60.winEXE@1/1@0/0
EGA Information:	• Successful, ratio: 100%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

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

C:\Users\user\AppData\Local\Temp\iext1.fnr.bbs.125.la

Process:	C:\Users\user\Desktop\YY#U6302#U53f7#U534f#U8bae.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	741376
Entropy (8bit):	6.917105002705599
Encrypted:	false
SSDEEP:	12288:wKBQAJdbyF+XZrjvhleWgtN5XcTXrTmY5GTTTTTTTTy8L1d8GsgFMwq:wKBZbpXZrjhI8N5sT7TzGTTTTTTTTy9
MD5:	A96FBD5E66B31F3D816AD80F623E9BD9
SHA1:	4EDA42260BD3EB930CD4EAFD7D15C6AF367BCF18
SHA-256:	2E67BA278646FDE95BB614DCBCC7DA1C6BF7976C918B2C6AD3D78640000326F3
SHA-512:	43921107313775EA14B1BD33CF758C13798F4FA1C1074771C1C96B1B43B98F3416D249ED8AB3171383772D0054829C3754A91B5E94135F1DF6D67A76F599C80E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....L.\|.....L.z....L.{.....H.....H.z./...H.{.....H.\|.....L.~.....~. .....w.H.....}.....Rich.....PE..L.....d.....!.."....r.....@.....@...T.....0.....@..`k.....p..... .....@.....P.....text..... ..`.rdata.....@..@.data...4.....@....detourc."......$.....@..@.de tourd..... .....@....rsrc.....0.....@..@.reloc..`k...@...I.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.921437760987104
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	YY#U6302#U53f7#U534f#U8bae.exe
File size:	4'972'544 bytes
MD5:	765cf453d0cea3719b619e4c55881093
SHA1:	060ae0476bbd908d08537c8b6bb24d2ec83d524c
SHA256:	3d76cc27be3265077a5c15f2c76848b73148df035b7d3a3d2b9ad77232587cfd
SHA512:	2132af60567aaf5c89001c36edd0764ef5e336dd2260d20287953ce2dac4b80c7817d0c0fe410a0d092900181c3d360999f7f2c06b5eba51a2e54821175cec18
SSDEEP:	98304:ygvElT54uia2kf5SCyJsAh6wbwPy7kl/CNBIs0lApvWJ:yFT54rHi4H+Ah/bOUkVQY2oJ
TLSH:	893633D84EF59834C2A6033CE43172374EBFF657D628936E265CE6AEAC4D1819341A37
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.vOB.%OB.%OB.%].%FB.%].%IB.%.^.%bB.%4^.%JB.%.].%cB.%.J.%MB.%OB.%.@.%-].%RB.%yd.%.B.%yd.%7B.%.].%.B.%.].%RB.%OB.%.B.%.D.%NB.

File Icon

Icon Hash:	099c9113582f8b55

Static PE Info

General

Entrypoint:	0xb93dda
Entrypoint Section:	.vmp1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x66653771 [Sun Jun 9 05:02:41 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	fe512f2e549df2214891378c91f66a42

Entrypoint Preview

Instruction
push 0E4B68F2h
call 00007F34FD55337Dh
add byte ptr [eax], al
push esp
insb
jnc 00007F34FD09BFE8h
jc 00007F34FD09C007h
add byte ptr [eax], al
add byte ptr [edi+65h], al
je 00007F34FD09BFF5h
jns 00007F34FD09C015h
je 00007F34FD09C007h
insd
push esp

Instruction
imul ebp, dword ptr [ebp+65h], 24648D00h
sbb al, E8h
popfd
add dword ptr [eax], eax
add byte ptr [ebx-18h], dl
lock add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [ebx+65h], dl
je 00007F34FD09BFF9h
imul ebp, dword ptr [esi+64h], 7845776Fh
je 00007F34FD09BFE7h
js 00007F34FD09BFA2h
add byte ptr [eax], al
inc edi
je 00007F34FD09BFF9h
outsd
insb
jne 00007F34FD09C00Fh
dec ecx
outsb
outsw
jc 00007F34FD09C00Fh
popad
je 00007F34FD09C00Bh
outsd
outsb
inc ecx
add byte ptr [eax], al
add byte ptr [ebx+72h], al
popad
je 00007F34FD09C007h
push esp
push 64616572h
add al, ch
pop esi
or al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [ebx+72h], al
popad
je 00007F34FD09C007h
inc esp
imul esi, dword ptr [edx+65h], 726F7463h
jns 00007F34FD09BFE3h
add byte ptr [eax], al
add byte ptr [edi+69h], dl
inc ebx
push 6F547261h
dec ebp
jne 00007F34FD09C00Eh
je 00007F34FD09C00Bh
inc edx
jns 00007F34FD09C016h
add byte ptr [eax], al
add byte ptr [edi+61h], dl
imul esi, dword ptr [esi+eax*2+6Fh], 6C754D72h
je 00007F34FD09C00Bh
jo 00007F34FD09C00Eh
dec edi
bound ebp, dword ptr [edx+65h]

Instruction
arpl word ptr [ebx+esi*2+00h], si
add byte ptr [eax], al
inc ecx
jo 00007F34FD09C012h
outsb
dec ebp
outsb
jne 00007F34FD09BFE3h
add byte ptr [eax], al
add byte ptr [ebx+72h], al
popad
je 00007F34FD09C007h

Rich Headers

Programming Language:	• [C] VS98 (6.0) SP6 build 8804 • [C++] VS98 (6.0) SP6 build 8804 • [C++] VS98 (6.0) build 8168 • [C] VS98 (6.0) build 8168 • [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x79627c	0x168	.vmp1
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x788000	0x6190	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4c000	0x4c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
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	0xb9735b	0x850	.vmp1
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19e742	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1a0000	0x577b12	0x0	d41d8cd98f00b204e9800998ecf8427e	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x718000	0x6f3ca	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x788000	0x6190	0x3000	a1864bf4c4f443ebfc78e5e2fff8348b	False	0.394287109375	data	4.088331277576032	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vmp0	0x78f000	0x3024	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.vmp1	0x793000	0x4b8233	0x4b9000	5d3194b71c1a11ae1687b1d9c64ef151	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0xc4c000	0x4c	0x1000	31b33e1e166e82486ce7540bf78125ec	False	0.0224609375	data	0.11968309355305998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
TEXTINCLUDE	0x78a5b8	0xb	data	Chinese	China	1.0
TEXTINCLUDE	0x78a5c4	0x16	data	Chinese	China	0.5
TEXTINCLUDE	0x78a5dc	0x151	data	Chinese	China	0.03857566765578635
RT_CURSOR	0x78a730	0x134	data	Chinese	China	0.04220779220779221
RT_CURSOR	0x78a864	0x134	data	Chinese	China	0.04220779220779221
RT_CURSOR	0x78a998	0x134	data	Chinese	China	0.04220779220779221
RT_CURSOR	0x78aacc	0xb4	data	Chinese	China	0.06666666666666667
RT_BITMAP	0x78ab80	0x16c	data	Chinese	China	0.03571428571428571
RT_BITMAP	0x78acec	0x248	data	Chinese	China	0.025684931506849314
RT_BITMAP	0x78af34	0x144	data	Chinese	China	0.058823529411764705
RT_BITMAP	0x78b078	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b1d0	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b328	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b480	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b5d8	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b730	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b888	0x158	empty	Chinese	China	0
RT_BITMAP	0x78b9e0	0x158	empty	Chinese	China	0
RT_BITMAP	0x78bb38	0x5e4	empty	Chinese	China	0
RT_BITMAP	0x78c11c	0xb8	empty	Chinese	China	0
RT_BITMAP	0x78c1d4	0x16c	empty	Chinese	China	0
RT_BITMAP	0x78c340	0x144	empty	Chinese	China	0
RT_ICON	0x788bf4	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	Chinese	China	0.26344086021505375
RT_ICON	0x788edc	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Chinese	China	0.41216216216216217
RT_ICON	0x789004	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0, resolution 2834 x 2834 px/m			0.6824577861163227
RT_MENU	0x78c484	0xc	empty	Chinese	China	0
RT_MENU	0x78c490	0x284	empty	Chinese	China	0
RT_DIALOG	0x78c714	0x98	empty	Chinese	China	0
RT_DIALOG	0x78c7ac	0x17a	empty	Chinese	China	0
RT_DIALOG	0x78c928	0xfa	empty	Chinese	China	0
RT_DIALOG	0x78ca24	0xea	empty	Chinese	China	0
RT_DIALOG	0x78cb10	0x8ae	empty	Chinese	China	0
RT_DIALOG	0x78d3c0	0xb2	empty	Chinese	China	0
RT_DIALOG	0x78d474	0xcc	empty	Chinese	China	0
RT_DIALOG	0x78d540	0xb2	empty	Chinese	China	0
RT_DIALOG	0x78d5f4	0xe2	empty	Chinese	China	0
RT_DIALOG	0x78d6d8	0x18c	empty	Chinese	China	0
RT_STRING	0x78d864	0x50	empty	Chinese	China	0
RT_STRING	0x78d8b4	0x2c	empty	Chinese	China	0
RT_STRING	0x78d8e0	0x78	empty	Chinese	China	0
RT_STRING	0x78d958	0x1c4	empty	Chinese	China	0
RT_STRING	0x78db1c	0x12a	empty	Chinese	China	0
RT_STRING	0x78dc48	0x146	empty	Chinese	China	0
RT_STRING	0x78dd90	0x40	empty	Chinese	China	0

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_STRING	0x78ddd0	0x64	empty	Chinese	China	0
RT_STRING	0x78de34	0x1d8	empty	Chinese	China	0
RT_STRING	0x78e00c	0x114	empty	Chinese	China	0
RT_STRING	0x78e120	0x24	empty	Chinese	China	0
RT_GROUP_CURSOR	0x78e144	0x14	empty	Chinese	China	0
RT_GROUP_CURSOR	0x78e158	0x14	empty	Chinese	China	0
RT_GROUP_CURSOR	0x78e16c	0x22	empty	Chinese	China	0
RT_GROUP_ICON	0x78a0ac	0x14	data			1.2
RT_GROUP_ICON	0x78a0c0	0x14	data	Chinese	China	1.2
RT_GROUP_ICON	0x78a0d4	0x14	data	Chinese	China	1.25
RT_VERSION	0x78a0e8	0x214	data	Chinese	China	0.5375939849624061
RT_MANIFEST	0x78a2fc	0x2b9	XML 1.0 document, ASCII text, with very long lines (697), with no line terminators			0.5279770444763271

Imports

DLL	Import
RASAPI32.dll	RasHangUpA, RasGetConnectStatusA
WINMM.dll	midiStreamRestart, midiStreamClose, midiOutReset, midiStreamStop, midiStreamOut, midiOutPrepareHeader, waveOutRestart, waveOutUnprepareHeader, waveOutPrepareHeader, waveOutWrite, waveOutPause, waveOutReset, midiStreamProperty, midiStreamOpen, midiOutUnprepareHeader, waveOutOpen, waveOutClose, waveOutGetNumDevs
WS2_32.dll	WSAAsyncSelect, closesocket, send, select, WSACleanup, WSAStartup, gethostbyname, inet_ntoa, inet_addr, gethostname, htons, socket, sendto, recvfrom, ioctlsocket, connect, listen, getpeername, accept, __WSAFDIsSet, ntohs, htonl, bind, ntohl, WSAGetLastError, getsockname, recv
KERNEL32.dll	UnmapViewOfFile, CreateFileMappingA, MapViewOfFile, OpenFileMappingA, GetCurrentProcessId, GetSystemDirectoryA, GetWindowsDirectoryA, GetCurrentProcess, TerminateThread, GetModuleHandleW, VirtualQuery, LoadLibraryW, GetVersionExW, DeleteFileW, TerminateProcess, GetFileSize, SetFilePointer, CreateFileW, GetTempPathW, FileTimeToSystemTime, GetTimeZoneInformation, SetLastError, GetVersion, LocalFree, FormatMessageA, CreateMutexA, ReleaseMutex, SuspendThread, GetACP, CreateSemaphoreA, ResumeThread, InterlockedExchange, ReleaseSemaphore, IsBadCodePtr, IsBadReadPtr, CompareStringW, CompareStringA, GetStringTypeW, GetStringTypeA, SetUnhandledExceptionFilter, IsBadWritePtr, VirtualAlloc, LCMapStringW, LCMapStringA, SetEnvironmentVariableA, VirtualFree, HeapCreate, HeapDestroy, GetEnvironmentVariableA, GetStdHandle, SetHandleCount, GetEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsW, FreeEnvironmentStringsA, UnhandledExceptionFilter, GetFileType, SetStdHandle, HeapSize, ExitThread, GetLocalTime, GetSystemTime, RaiseException, RtlUnwind, GetStartupInfoA, GetOEMCP, GetCPInfo, GetProcessVersion, SetErrorMode, GlobalFlags, GetCurrentThread, GetFileTime, TlsGetValue, LocalReAlloc, TlsSetValue, TlsFree, GlobalHandle, TlsAlloc, LocalAlloc, lstrcmpA, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, GlobalDeleteAtom, lstrcmpiA, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, DuplicateHandle, lstrcpynA, FileTimeToLocalFileTime, InterlockedDecrement, InterlockedIncrement, EnterCriticalSection, LeaveCriticalSection, GetProfileStringA, WriteFile, WaitForMultipleObjects, CloseHandle, WaitForSingleObject, CreateProcessA, GetTickCount, GetCommandLineA, MulDiv, GetProcAddress, GetModuleHandleA, GetVolumeInformationA, SetCurrentDirectoryA, GetCurrentDirectoryA, CreateDirectoryA, CopyFileA, DeleteFileA, GetFileAttributesA, SetFileAttributesA, FindClose, FindFirstFileA, GetTempPathA, CreateFileA, SetEvent, FindResourceA, LoadResource, LockResource, ReadFile, lstrlenW, RemoveDirectoryA, GetModuleFileNameA, GetCurrentThreadId, ExitProcess, GlobalSize, GlobalFree, DeleteCriticalSection, InitializeCriticalSection, lstrcatA, lstrlenA, WinExec, lstrcpyA, FindNextFileA, GlobalReAlloc, HeapFree, HeapReAlloc, GetProcessHeap, HeapAlloc, GetUserDefaultLCID, MultiByteToWideChar, WideCharToMultiByte, GetFullPathNameA, FreeLibrary, LoadLibraryA, GetLastError, GetVersionExA, WritePrivateProfileStringA, GetPrivateProfileStringA, CreateThread, CreateEventA, Sleep, GlobalAlloc, GlobalLock, GlobalUnlock
USER32.dll	GetClassNameA, GetDesktopWindow, GetDlgItem, SetWindowTextA, MessageBoxW, GetSysColorBrush, wsprintfA, WaitForInputIdle, FindWindowExA, GetWindowTextA, ReleaseDC, LoadStringA, GetMenuCheckMarkDimensions, GetMenuState, SetMenuItemBitmaps, CheckMenuItem, MoveWindow, GetForegroundWindow, DefWindowProcW, GetPropA, RegisterClassA, CreateWindowExA, SetPropA, LoadIconA, TranslateMessage, DrawFrameControl, DrawEdge, DrawFocusRect, WindowFromPoint, GetMessageA, DispatchMessageA, SetRectEmpty, RegisterClipboardFormatA, CreateIconFromResourceEx, CreateIconFromResource, DrawIconEx, CreatePopupMenu, AppendMenuA, ModifyMenuA, CreateMenu, CreateAcceleratorTableA, GetDlgCtrlID, GetSubMenu, EnableMenuItem, ClientToScreen, EnumDisplaySettingsA, LoadImageA, SystemParametersInfoA, ShowWindow, IsWindowEnabled, TranslateAcceleratorA, IsDialogMessageA, ScrollWindowEx, SendDlgItemMessageA, MapWindowPoints, AdjustWindowRectEx, GetScrollPos, GetMenuItemCount, GetMenuItemID, SetWindowsHookExA, CallNextHookEx, GetClassLongA, UnhookWindowsHookEx, CallWindowProcA, RemovePropA, GetMessageTime, GetLastActivePopup, RegisterWindowMessageA, GetWindowPlacement, GetNextDlgTabItem, EndDialog, CreateDialogIndirectParamA, DestroyWindow, GrayStringA, DrawTextA, TabbedTextOutA, EndPaint, BeginPaint, GetWindowDC, CharUpperA, GetWindowTextLengthA, GetKeyState, CopyAcceleratorTableA, PostQuitMessage, IsZoomed, GetClassInfoA, DefWindowProcA, GetSystemMenu, DeleteMenu, GetMenu, SetMenu, PeekMessageA, IsIconic, SetFocus, GetActiveWindow, GetWindow, DestroyAcceleratorTable, SetWindowRgn, GetMessagePos, ScreenToClient, ChildWindowFromPointEx, CopyRect, LoadBitmapA, WinHelpA, KillTimer, SetTimer, ReleaseCapture, GetCapture, SetCapture, GetScrollRange, SetScrollRange, SetScrollPos, SetRect, InflateRect, IntersectRect, DestroyIcon, PtInRect, OffsetRect, IsWindowVisible, EnableWindow, RedrawWindow, GetWindowLongA, SetWindowLongA, GetSysColor, SetActiveWindow, SetCursorPos, LoadCursorA, SetCursor, GetDC, FillRect, IsRectEmpty, UnregisterClassA, IsChild, TrackPopupMenu, DestroyMenu, SetForegroundWindow, GetWindowRect, EqualRect, UpdateWindow, ValidateRect, InvalidateRect, GetClientRect, GetFocus, GetParent, GetTopWindow, PostMessageA, IsWindow, SetParent, DestroyCursor, SendMessageA, SetWindowPos, MessageBoxA, GetCursorPos, GetSystemMetrics, EmptyClipboard, SetClipboardData, OpenClipboard, GetClipboardData, CloseClipboard

DLL	Import
GDI32.dll	ExtSelectClipRgn, LineTo, MoveToEx, ExcludeClipRect, GetClipBox, ScaleWindowExtEx, SetWindowExtEx, SetWindowOrgEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SetMapMode, SetTextColor, SetROP2, SetPolyFillMode, SetBkMode, SelectClipRgn, DeleteObject, CreateDIBitmap, GetSystemPaletteEntries, SelectPalette, RealizePalette, GetDIBits, GetWindowExtEx, GetViewportOrgEx, GetWindowOrgEx, BeginPath, EndPath, PathToRegion, CreateEllipticRgn, CreateRoundRectRgn, GetTextColor, GetBkMode, GetBkColor, GetROP2, GetStretchBltMode, GetPolyFillMode, CreateCompatibleBitmap, CreateDCA, CreateBitmap, SelectObject, CreatePen, PatBlt, CombineRgn, CreateRectRgn, FillRgn, CreateSolidBrush, CreateFontIndirectA, GetStockObject, GetObjectA, EndPage, EndDoc, DeleteDC, StartDocA, StartPage, BitBlt, CreateCompatibleDC, Ellipse, Rectangle, LPtoDP, DPtoLP, GetCurrentObject, RoundRect, GetTextExtentPoint32A, GetDeviceCaps, GetViewportExtEx, PtVisible, RectVisible, TextOutA, ExtTextOutA, Escape, GetTextMetricsA, CreatePolygonRgn, GetClipRgn, SetStretchBltMode, CreateRectRgnIndirect, SetBkColor, CreatePalette, StretchBlt, SaveDC, RestoreDC
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter
ADVAPI32.dll	RegSetValueExA, RegOpenKeyExA, RegCloseKey, RegQueryValueA, CryptReleaseContext, CryptDestroyHash, CryptGetHashParam, CryptHashData, CryptCreateHash, CryptAcquireContextA, RegCreateKeyExA
SHELL32.dll	DragQueryFileA, SHGetSpecialFolderPathA, Shell_NotifyIconA, ShellExecuteA
ole32.dll	OleRun, CoCreateInstance, CLSIDFromString, OleUninitialize, OleInitialize, RegisterDragDrop, RevokeDragDrop, ReleaseStgMedium, CLSIDFromProgID
OLEAUT32.dll	SafeArrayAccessData, SafeArrayGetElement, VariantCopyInd, VariantInit, SysAllocString, SafeArrayDestroy, SafeArrayCreate, SafeArrayPutElement, RegisterTypeLib, LHashValOfNameSys, LoadTypeLib, SafeArrayUnaccessData, UnRegisterTypeLib, SafeArrayGetDim, SafeArrayGetLBound, SafeArrayGetUBound, VariantChangeType, VariantClear, VariantCopy
COMCTL32.dll	ImageList_Destroy
WLDAP32.dll	
WININET.dll	InternetCanonicalizeUrlA, InternetCrackUrlA, HttpOpenRequestA, HttpSendRequestA, HttpQueryInfoA, InternetReadFile, InternetConnectA, InternetSetOptionA, InternetCloseHandle, InternetOpenA
comdlg32.dll	ChooseColorA, ChooseFontA, GetFileTitleA, GetSaveFileNameA, GetOpenFileNameA
KERNEL32.dll	VirtualProtect, GetModuleFileNameA, ExitProcess
USER32.dll	MessageBoxA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: YY#U6302#U53f7#U534f#U8bae.exe PID: **908**, Parent PID: **2580**

General

Target ID:	0
Start time:	14:02:56
Start date:	15/06/2024
Path:	C:\Users\user\Desktop\YY#U6302#U53f7#U534f#U8bae.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\YY#U6302#U53f7#U534f#U8bae.exe"
Imagebase:	0x400000
File size:	4'972'544 bytes
MD5 hash:	765CF453D0CEA3719B619E4C55881093
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iext1.fnr.bbs.125.la	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	53B714	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iext1.fnr.bbs.125.la	0	741376	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 43 fd 11 fd 07 fd 7f fd 07 fd 7f fd 07 fd 7f fd 4c fd 7c fd 09 fd 7f fd 4c fd 7a 28 fd 7f fd 4c fd 7b fd 11 fd 7f fd 48 c2 fd 02 fd 7f fd 48 fd 7a fd 2f fd 7f fd 48 fd 7b fd 16 fd 7f fd 48 fd 7c fd 12 fd 7f fd 4c fd 7e fd 08 fd 7f fd 07 fd 7e fd fd fd 7f fd fd fd 77 fd 48 fd 7f fd fd fd 7f fd 06 fd 7f fd fd c0 fd 06 fd 7f fd fd fd 7d fd 06 fd 7f fd 52 69 63 68 07 fd 7f	MZ@!L!This program cannot be run in DOS mode.$CL|LzL{HHz/H{H |L~~wH}Rich	success or wait	1	53B7CB	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly