ID: 679116
Sample Name: 22o5gJzlg6.exe
Cookbook: default.jbs
Time: 09:36:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

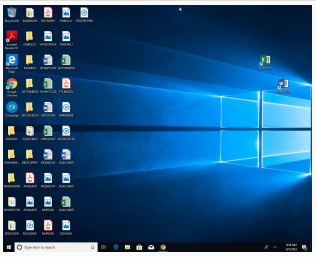
Windows Analysis Report

22o5gJzlg6.exe

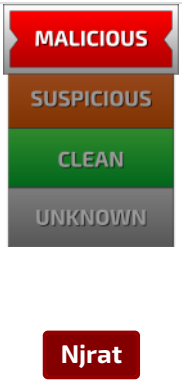
Overview

General Information

Sample Name:	22o5gJzlg6.exe
Analysis ID:	679116
MD5:	1f85c12fcd3232c..
SHA1:	3741755f8a1163..
SHA256:	f229ed07a73bf6f..
Tags:	exe njrat RAT
Infos:	



Detection



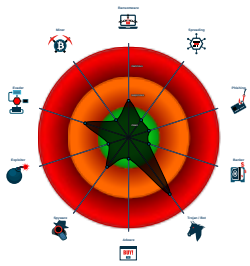
Njrat

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Njrat
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware con…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- PE file contains strange resources

Classification



Process Tree

- **System is w10x64**
- 22o5gJzlg6.exe (PID: 5776 cmdline: "C:\Users\user\Desktop\22o5gJzlg6.exe" MD5: 1F85C12FCD3232C577E5E8CC07FBF1E1)
- **cleanup**

Malware Configuration

Threatname: Njrat


```
{
  "Host": "milla11.publicvm.com",
  "Port": "5050",
  "Mutex Name": "d84c416188f84fa099",
  "Network Seprator": "@!#&^%$",
  "Campaign ID": "NYAN CAT",
  "Version": "0.7NC"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: 22o5gJzlg6.exe PID: 5776	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act) - Source IP: 192.168.2.5 - Destination IP: 91.109.186.4	
Timestamp:	192.168.2.591.109.186.44976550502825564 08/05/22-09:39:04.872116
SID:	2825564
Source Port:	49765
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.5 - Destination IP: 91.109.186.4	
Timestamp:	192.168.2.591.109.186.44976550502825563 08/05/22-09:37:42.892210
SID:	2825563
Source Port:	49765
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.5 - Destination IP: 91.109.186.4	
Timestamp:	192.168.2.591.109.186.44976550502033132 08/05/22-09:37:42.798572
SID:	2033132
Source Port:	49765
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Yara detected Njrat
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected Njrat

Stealing of Sensitive Information

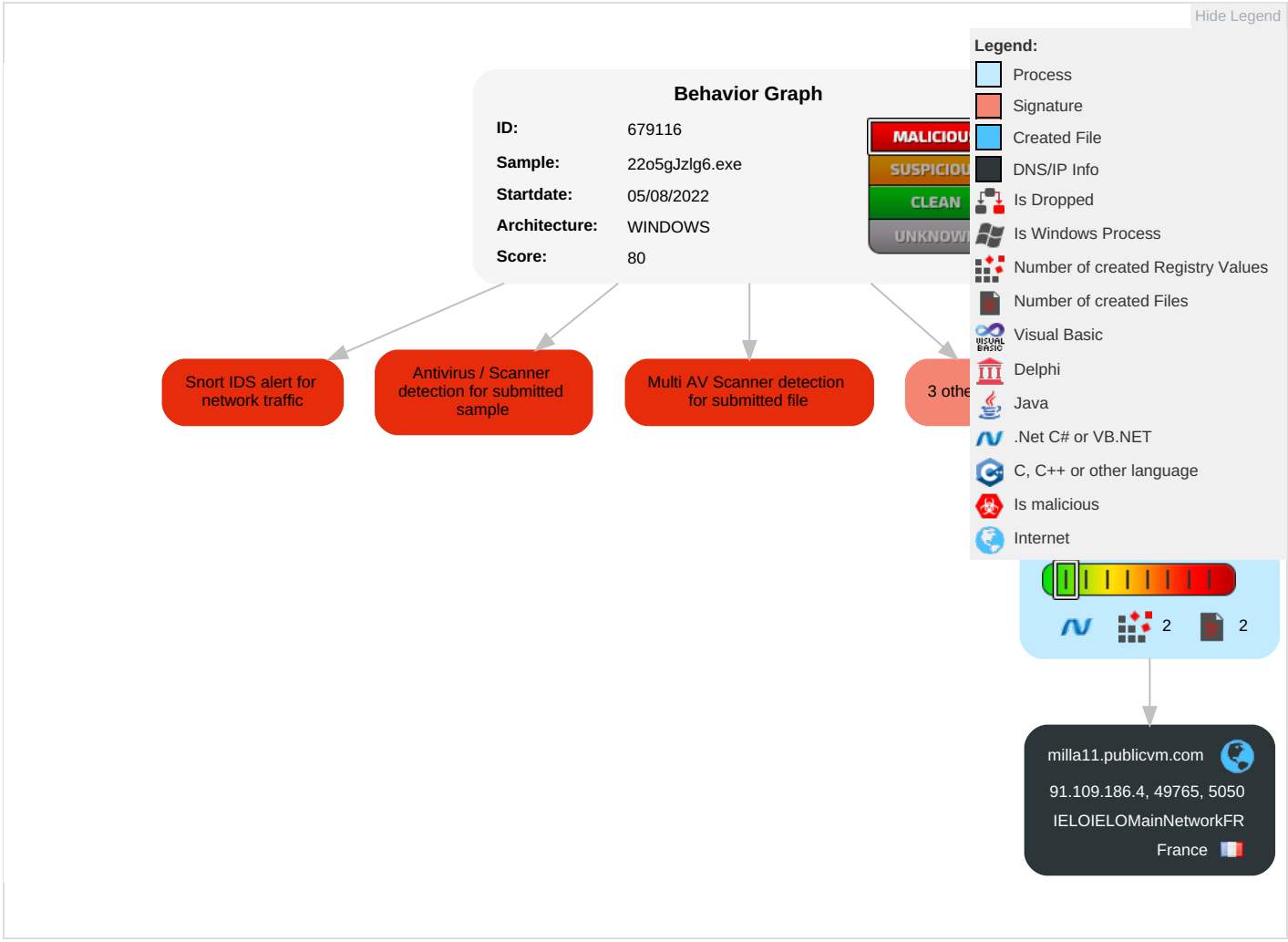
- Yara detected Njrat

Yara detected Njrat

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	1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Virtualization/Sandbox Evasion	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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

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
22o5gJzlg6.exe	73%	Virustotal		Browse
22o5gJzlg6.exe	43%	Metadefender		Browse
22o5gJzlg6.exe	69%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
22o5gJzlg6.exe	100%	Avira	TR/Dropper.MSIL.Gen	
22o5gJzlg6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.22o5gJzlg6.exe.430000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnQ	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.founder.com.cn/cnCTI	0%	Avira URL Cloud	safe	
http://www.carterandcone.com1	0%	URL Reputation	safe	
http://www.founder.com.cn/cnRIN	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comuea	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn.i	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTF	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/kurs	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.monotype.Y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/=	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/l	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comessedI	0%	Avira URL Cloud	safe	
http://www.carterandcone.comE	0%	URL Reputation	safe	
http://fontfabrik.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnTFu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.carterandcone.com8	0%	URL Reputation	safe	
http://www.fontbureau.com4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comC~	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/;	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.fontbureau.comtt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma-d	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comsiefl	0%	Avira URL Cloud	safe	
http://www.sakkal.com8	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html~	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kra	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://fontfabrik.com-e	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnva	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/iv	0%	Avira URL Cloud	safe	
http://www.carterandcone.com~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.fontbureau.comz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/sv-s	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comitu_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comT.TTF=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
milla11.publicvm.com	91.109.186.4	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
milla11.publicvm.com	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnQ	22o5gJzlg6.exe, 00000000.00000003.431386511.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431226577.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431148925.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431016693.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431510900.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comva	22o5gJzlg6.exe, 00000000.00000003.432499311.000000000580F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnCTI	22o5gJzlg6.exe, 00000000.00000003.430863609.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com1	22o5gJzlg6.exe, 00000000.00000003.432436607.0000000005811000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnRIN	22o5gJzlg6.exe, 00000000.00000003.430863609.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comuea	22o5gJzlg6.exe, 00000000.00000002.699727274.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446329043.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446126364.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446267888.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446363357.0000000005810000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn.i	22o5gJzlg6.exe, 00000000.00000003.432071419.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comTTF	22o5gJzlg6.exe, 00000000.00000003.437693822.000000000580E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessed	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438683013.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439187961.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439519748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438563728.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438487330.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439221383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438377965.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438456044.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439416035.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439279849.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/4	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/kurs	22o5gJzlg6.exe, 00000000.00000003.434060485.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434026409.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	22o5gJzlg6.exe, 00000000.00000003.430244973.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	22o5gJzlg6.exe, 00000000.00000003.432863626.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432436607.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432261621.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432675327.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432828022.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432499311.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432899886.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432630198.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433019323.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432759453.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432283139.000000000580F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnC	22o5gJzlg6.exe, 00000000.00000003.431148925.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431016693.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.Y	22o5gJzlg6.exe, 00000000.00000003.443332430.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/=	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/l	22o5gJzlg6.exe, 00000000.00000003.442520590.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442128327.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	22o5gJzlg6.exe, 00000000.00000003.442056543.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442655517.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442501394.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.428170416.0000000005806000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessedI	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438683013.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439187961.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438563728.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438487330.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438225069.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439221383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438377965.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438456044.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438174770.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439279849.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comE	22o5gJzlg6.exe, 00000000.00000003.432997847.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comx	22o5gJzlg6.exe, 00000000.00000003.428170416.0000000005806000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnTFu	22o5gJzlg6.exe, 00000000.00000003.430863609.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/4	22o5gJzlg6.exe, 00000000.00000003.434060485.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434026409.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com8	22o5gJzlg6.exe, 00000000.00000003.433244896.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432997847.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com4	22o5gJzlg6.exe, 00000000.00000003.439609629.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439519748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439279849.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//	22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435402188.000000000581200.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comrsiv&	22o5gJzlg6.exe, 00000000.00000003.440822748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.000000000581200.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440850654.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.000000000581200.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.000000000581200.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.000000000581200.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/(	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.000000000581000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	22o5gJzlg6.exe, 00000000.00000003.427915980.000000005806000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	22o5gJzlg6.exe, 00000000.00000003.430432412.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430522948.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430486289.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430185630.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430244973.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430578626.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/&	22o5gJzlg6.exe, 00000000.00000003.435442221.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.436179663.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435352161.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435573925.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435635608.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.436098101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435840977.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.436041454.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435402188.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432261621.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432071419.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.	22o5gJzlg6.exe, 00000000.00000003.432675327.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432828022.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432630198.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432759453.000000000580F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comC~	22o5gJzlg6.exe, 00000000.00000003.432863626.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433296887.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433244896.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432997847.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433420738.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/;	22o5gJzlg6.exe, 00000000.00000003.430476742.0000000005806000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430516625.0000000005806000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coma	22o5gJzlg6.exe, 00000000.00000003.433296887.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433244896.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432997847.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433420738.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440146087.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.437770989.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438683013.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440822748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439187961.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.000000000581200 0.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438563728.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440850654.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438487330.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438225069.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439221383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438377965.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438456044.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/	22o5gJzlg6.exe, 00000000.00000003.442920288.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442005981.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442520590.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443542427.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442655517.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443031431.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442962847.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442741235.000000000581200 0.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443220777.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.442128327.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443153111.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443450897.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.443332430.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/X	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	22o5gJzlg6.exe, 00000000.00000003.437693822.000000000580E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/V	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comtt	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438683013.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439187961.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438563728.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438487330.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438225069.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439221383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438377965.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438456044.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439279849.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd_	22o5gJzlg6.exe, 00000000.00000003.438683013.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438563728.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438487330.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438225069.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438377965.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438456044.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438174770.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/	22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.436098101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435840977.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.436041454.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435402188.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	22o5gJzlg6.exe, 00000000.00000003.437851582.000000000580E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coma-d	22o5gJzlg6.exe, 00000000.00000003.432261621.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	22o5gJzlg6.exe, 00000000.00000003.440146087.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440822748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439609629.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440850654.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439642692.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsiefl	22o5gJzlg6.exe, 00000000.00000003.440146087.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440822748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440850654.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com8	22o5gJzlg6.exe, 00000000.00000003.435143246.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435173659.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html~	22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435352161.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435564805.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435393505.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435434677.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kra	22o5gJzlg6.exe, 00000000.00000003.430432412.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.430486289.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	22o5gJzlg6.exe, 00000000.00000003.427915980.0000000005806000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

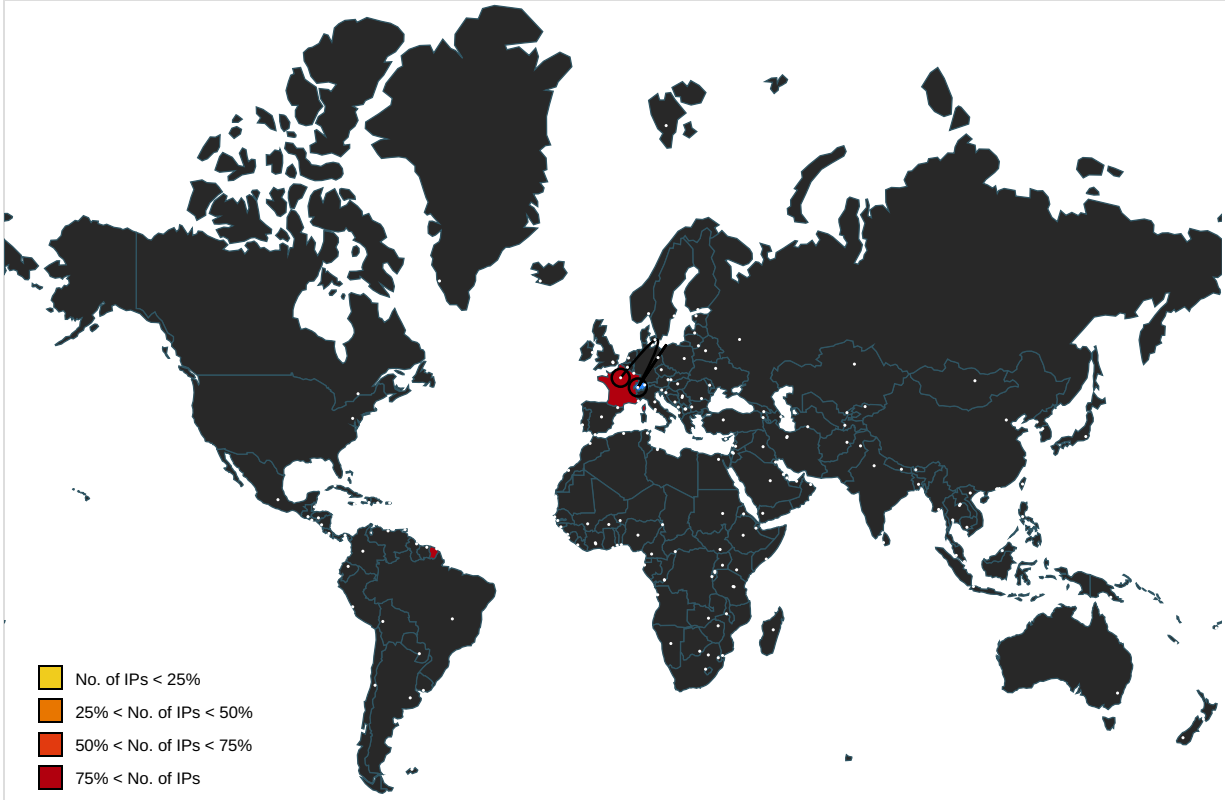
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/=	22o5gJzlg6.exe, 00000000.00000003.434060485.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434026409.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	22o5gJzlg6.exe, 00000000.00000002.699831067.00000000069F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	22o5gJzlg6.exe, 00000000.00000003.431386511.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431226577.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431719100.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431510900.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	22o5gJzlg6.exe, 00000000.00000003.431016693.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.431510900.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com-e	22o5gJzlg6.exe, 00000000.00000003.428170416.0000000005806000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	22o5gJzlg6.exe, 00000000.00000003.438782064.00000000057F0000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnva	22o5gJzlg6.exe, 00000000.00000003.432436607.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432071419.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432283139.000000000580F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/r	22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	22o5gJzlg6.exe, 00000000.00000003.445348164.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.445413832.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.441424361.00000000057EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comt	22o5gJzlg6.exe, 00000000.00000002.699727274.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446329043.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446126364.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446267888.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.446363357.0000000005810000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/iv	22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com~	22o5gJzlg6.exe, 00000000.00000003.432863626.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.433244896.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432997847.0000000005808000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comm	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439187961.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439279849.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/l	22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.00000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comz	22o5gJzlg6.exe, 00000000.00000003.437851582.000000000580E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/sv-s	22o5gJzlg6.exe, 00000000.00000003.435183566.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434705101.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435226866.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435154857.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434492066.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434965433.00000000058010000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434616172.0000000005810000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434929567.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434860772.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.435275521.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.434381509.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.	22o5gJzlg6.exe, 00000000.00000003.432436607.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432071419.0000000005808000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432499311.000000000580F000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.432283139.000000000580F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	22o5gJzlg6.exe, 00000000.00000002.700212667.0000000006AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	22o5gJzlg6.exe, 00000000.00000003.440146087.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439609629.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439642692.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.00000000058000D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comitu_	22o5gJzlg6.exe, 00000000.00000003.440146087.0000000005811000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440822748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439609629.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440351183.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439519748.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440850654.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440448532.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.439642692.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440257383.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440546293.0000000005812000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.440646134.0000000005812000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comT.TTF=	22o5gJzlg6.exe, 00000000.00000003.439066250.000000000580E000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438952936.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438892084.000000000580D000.00000004.00000800.00020000.00000000.sdmp, 22o5gJzlg6.exe, 00000000.00000003.438763045.000000000580D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.109.186.4	milla11.publicvm.com	France		29075	IELOIELOMainNetworkFR	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679116
Start date and time: 05/08/202209:36:11	2022-08-05 09:36:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	22o5gJzlg6.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:	18
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:	mal80.troj.winEXE@1/0@1/1
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: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-azurecdn-akamai-iris.azureedge.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target 22o5gJzlg6.exe, PID 5776 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey 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):	7.014106369522473
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	22o5gJzlg6.exe
File size:	772608
MD5:	1f85c12fcd3232c577e5e8cc07fbf1e1
SHA1:	3741755f8a11638209821a3cd7c01104acac184d
SHA256:	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4
SHA512:	9a991ea8dd19bff6a7a83d546b2f4d958e849a17ef4cbc62c2faaf3e9588fc896c7cd48fe76cfa34a2efa66327002fb412201d32e74a5c683c30ee1fe1138667
SSDEEP:	12288:WqShIfQIKMR4LClwugCEzE3qA2nv1gfckf:4hIYIKMCigCEzE312nKck
TLSH:	4DF4920B5D78868AE1FA3530C6F670B3A273970BDD098A35697DE0C37E29DE904E7116
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$..b.....3... ...@....@.. ....

File Icon

Icon Hash:	f8c6e86968b0cc70

Static PE Info

General

Entrypoint:	0x4933ee
Entrypoint Section:	.text
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:	0x62E8FC24 [Tue Aug 2 10:27:48 2022 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:	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

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
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	0x93394	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0x2b198	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	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	0x913f4	0x91400	False	0.7046612790447504	data	7.472442868082026	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x94000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x2b198	0x2b200	False	0.17342617753623188	data	3.676783822364216	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x962b0	0x31c8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x99478	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xa9ca0	0x94a8	data		
RT_ICON	0xb3148	0x5488	data		
RT_ICON	0xb85d0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 64767, next used block 4282318848		
RT_ICON	0xbc7f8	0x25a8	data		
RT_ICON	0xbeda0	0x10a8	data		
RT_ICON	0xbfe48	0x988	data		
RT_ICON	0xc07d0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc0c38	0x84	data		
RT_VERSION	0xc0cbc	0x2f0	SysEx File - IDP		
RT_MANIFEST	0xc0fac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

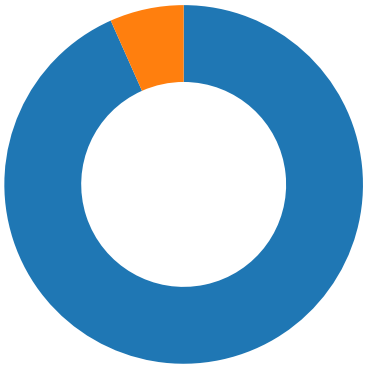
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.591.109.186.44976550502825564 08/05/22-09:39:04.872116	TCP	2825564	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)	49765	5050	192.168.2.5	91.109.186.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.591.109.186.44 976550502825563 08/05/22-09:37:42.892210	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49765	5050	192.168.2.5	91.109.186.4
192.168.2.591.109.186.44 976550502033132 08/05/22-09:37:42.798572	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49765	5050	192.168.2.5	91.109.186.4

Network Port Distribution



Total Packets: 15

- 53 (DNS)
- 5050 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:37:41.568679094 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:41.630243063 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:37:41.630374908 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:42.798572063 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:42.892086983 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:37:42.892210007 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:42.985652924 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:37:47.422403097 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:47.517601013 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:37:47.720798969 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:37:47.723356962 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:37:47.818135023 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:05.765523911 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:05.766052961 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:38:05.856589079 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:23.812676907 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:23.814517975 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:38:23.905464888 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:41.821995974 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:41.822762012 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:38:41.916249990 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:56.442615032 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:38:56.534531116 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:59.864129066 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:38:59.864787102 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:38:59.956043959 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:39:04.872116089 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:39:04.967768908 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:39:17.911744118 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:39:17.942150116 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:39:18.130026102 CEST	5050	49765	91.109.186.4	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:39:35.925879955 CEST	5050	49765	91.109.186.4	192.168.2.5
Aug 5, 2022 09:39:35.926232100 CEST	49765	5050	192.168.2.5	91.109.186.4
Aug 5, 2022 09:39:36.021418095 CEST	5050	49765	91.109.186.4	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:37:41.422647953 CEST	61356	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:37:41.550160885 CEST	53	61356	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:37:41.422647953 CEST	192.168.2.5	8.8.8.8	0x2963	Standard query (0)	milla11.publicvm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:37:41.550160885 CEST	8.8.8.8	192.168.2.5	0x2963	No error (0)	milla11.publicvm.com		91.109.186.4	A (IP address)	IN (0x0001)

Statistics

No statistics

System Behavior

Analysis Process: 22o5gJzlg6.exe PID: 5776, Parent PID: 5648

General

Target ID:	0
Start time:	09:37:20
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\22o5gJzlg6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\22o5gJzlg6.exe"
Imagebase:	0x430000
File size:	772608 bytes
MD5 hash:	1F85C12FCD3232C577E5E8CC07FBF1E1
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	6D89CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D89CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D875705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D87CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6E1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\d84c416188f84fa099	success or wait	1	6C6E5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	6C6E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\d84c416188f84fa099	[kl]	unicode		success or wait	1	6C6E646A	RegSetValueExW

Disassembly

No disassembly