ID: 358589
Sample Name: Setup.exe
Cookbook: default.jbs
Time: 21:57:47
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Setup.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Analysis Advice 5
Startup 5
Malware Configuration 6
Yara Overview 6
Sigma Overview 6
Signature Overview 6
Compliance: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
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 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 20
General 20
File Icon 20
Static PE Info 20
General 20
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 22
Resources 22
Imports 24
Version Infos 24
Possible Origin 25
Network Behavior 25
UDP Packets 25

Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: Setup.exe PID: 6588 Parent PID: 5704 26
General 26
File Activities 27
File Created 27
File Deleted 29
File Written 29
File Read 32
Analysis Process: svchost.exe PID: 6600 Parent PID: 568 33
General 33
File Activities 33
Analysis Process: msiexec.exe PID: 6708 Parent PID: 6588 33
General 33
File Activities 34
Analysis Process: msiexec.exe PID: 6764 Parent PID: 2224 34
General 34
Analysis Process: msiexec.exe PID: 7052 Parent PID: 2224 34
General 34
Analysis Process: CloudHttpWin32Server.exe PID: 7100 Parent PID: 568 34
General 34
File Activities 35
Analysis Process: cmd.exe PID: 7120 Parent PID: 7100 35
General 35
File Activities 35
Analysis Process: conhost.exe PID: 7148 Parent PID: 7120 35
General 35
Analysis Process: taskkill.exe PID: 6100 Parent PID: 7120 35
General 35
File Activities 36
Analysis Process: cmd.exe PID: 5364 Parent PID: 7100 36
General 36
File Activities 36
Analysis Process: conhost.exe PID: 4084 Parent PID: 5364 36
General 36
Analysis Process: taskkill.exe PID: 1004 Parent PID: 5364 36
General 36
File Activities 37
Analysis Process: CloudHttpServer.exe PID: 1636 Parent PID: 7100 37
General 37
File Activities 37
Analysis Process: CloudHttpWindowPopup.exe PID: 6052 Parent PID: 7100 37
General 37
File Activities 37
Analysis Process: conhost.exe PID: 6312 Parent PID: 1636 38
General 38
Analysis Process: conhost.exe PID: 6224 Parent PID: 6052 38
General 38
Analysis Process: cmd.exe PID: 3980 Parent PID: 7100 38
General 38
File Activities 38
Analysis Process: conhost.exe PID: 2992 Parent PID: 3980 39
General 39
Analysis Process: taskkill.exe PID: 6184 Parent PID: 3980 39
General 39
File Activities 39
Analysis Process: cmd.exe PID: 6152 Parent PID: 7100 39
General 39
File Activities 39
Analysis Process: conhost.exe PID: 6208 Parent PID: 6152 40
General 40
Analysis Process: taskkill.exe PID: 6404 Parent PID: 6152 40
General 40
File Activities 40
Analysis Process: svchost.exe PID: 6340 Parent PID: 568 40
General 40
File Activities 40

Registry Activities 41
Analysis Process: svchost.exe PID: 6724 Parent PID: 568 41
General 41
File Activities 41
Analysis Process: svchost.exe PID: 7012 Parent PID: 568 41
General 41
Analysis Process: svchost.exe PID: 7032 Parent PID: 568 41
General 41
File Activities 42
Analysis Process: svchost.exe PID: 5324 Parent PID: 568 42
General 42
File Activities 42
Analysis Process: svchost.exe PID: 4472 Parent PID: 568 42
General 42
Registry Activities 42
Analysis Process: svchost.exe PID: 6104 Parent PID: 568 43
General 43
Analysis Process: SgrmBroker.exe PID: 1744 Parent PID: 568 43
General 43
Analysis Process: svchost.exe PID: 5368 Parent PID: 568 43
General 43
Analysis Process: svchost.exe PID: 6172 Parent PID: 568 43
General 43
Disassembly 44
Code Analysis 44

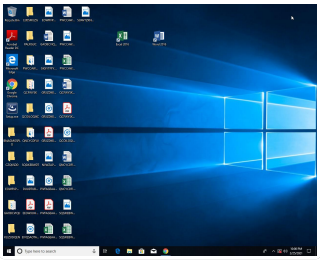
Analysis Report Setup.exe

Overview

General Information

Sample Name:	Setup.exe
Analysis ID:	358589
MD5:	7b5d30bd9b7cdc..
SHA1:	45fe889c3660be6.
SHA256:	a6385ebfc0c6e76..
Infos:	

Most interesting Screenshot:



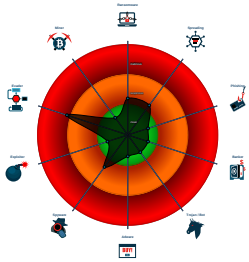
Detection

Score:	24
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Changes security center settings (no…
- AV process strings found (often use…
- Checks for available system drives …
- Checks if Antivirus/Antispyware/Fire…
- Contains functionality to dynamically…
- Contains functionality to query locale…
- Contains functionality to shutdown / …
- Contains functionality which may be…
- Creates a process in suspended mo…
- Creates files inside the system direc…
- Detected potential crypto function
- Drops PE files
- Enables debug privileges

Classification



Analysis Advice

- **Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook**
- **Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")**
- **Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior**

Startup

- **System is w10x64**
- Setup.exe (PID: 6588 cmdline: 'C:\Users\user\Desktop\Setup.exe' MD5: 7B5D30BD9B7CDCCA79E189AAAF5707FA)
  - msiexec.exe (PID: 6708 cmdline: MSIEXEC.EXE /i 'C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi' SETUPEXEDIR='C:\Users\user\Desktop' SETUPEXENAME='Setup.exe' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- svchost.exe (PID: 6600 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- msiexec.exe (PID: 6764 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding C31728C15F7B7E0360F95AF524D72042 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- msiexec.exe (PID: 7052 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 9ADD54B1DEB9106D315583847C272BCA MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- CloudHttpWin32Server.exe (PID: 7100 cmdline: C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWin32Server.exe MD5: 5921172EC58195BD404999F1D46A6867)
  - cmd.exe (PID: 7120 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpServer.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6100 cmdline: taskkill /F /IM CloudHttpServer.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
  - cmd.exe (PID: 5364 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpWindowPopup.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 1004 cmdline: taskkill /F /IM CloudHttpWindowPopup.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
  - CloudHttpServer.exe (PID: 1636 cmdline: C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpServer.exe MD5: FC73EBB8FB9E3B9520CE0516E778B6B9)
    - conhost.exe (PID: 6312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CloudHttpWindowPopup.exe (PID: 6052 cmdline: C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWindowPopup.exe MD5: C67AA650D57D92A0CF805343593C6AB9)
    - conhost.exe (PID: 6224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3980 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpServer.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6184 cmdline: taskkill /F /IM CloudHttpServer.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
  - cmd.exe (PID: 6152 cmdline: C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpWindowPopup.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6404 cmdline: taskkill /F /IM CloudHttpWindowPopup.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- svchost.exe (PID: 6340 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6724 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7012 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7032 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5324 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4472 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6104 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1744 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5368 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6172 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

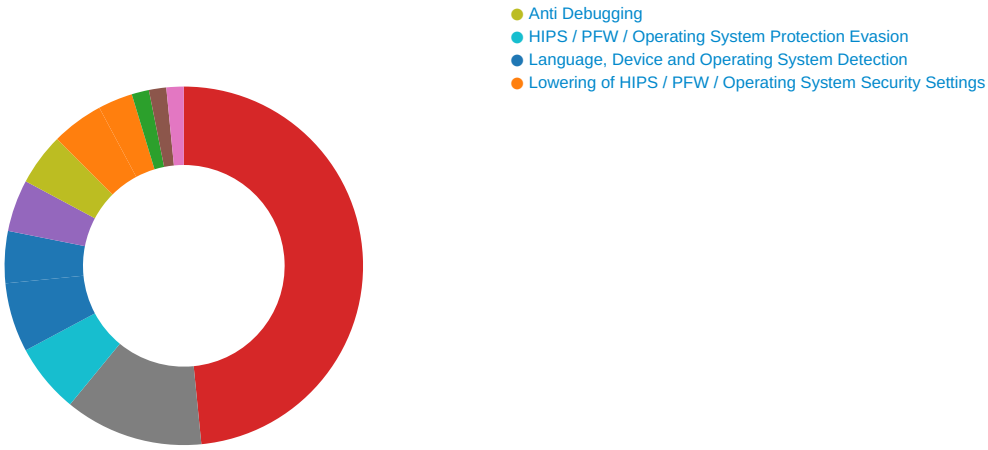
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion



Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Binary contains paths to debug symbols

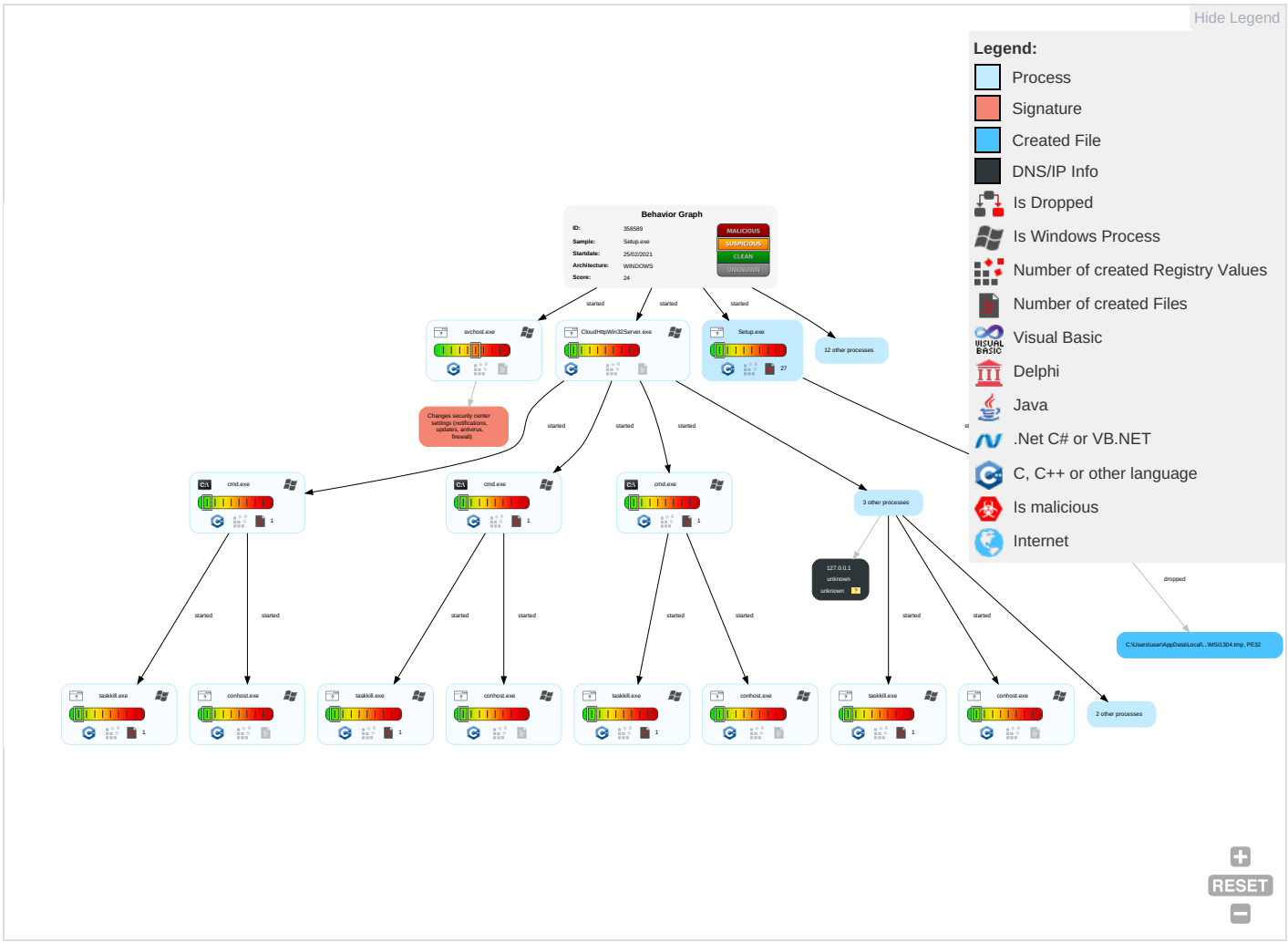
Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Replication Through Removable Media 1	Windows Management Instrumentation 1 1	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1 2	OS Credential Dumping	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Con
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Process Injection 1 2	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exp Red Call
Domain Accounts	Native API 2	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exp Trac Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Peripheral Device Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Con
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 3 7	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

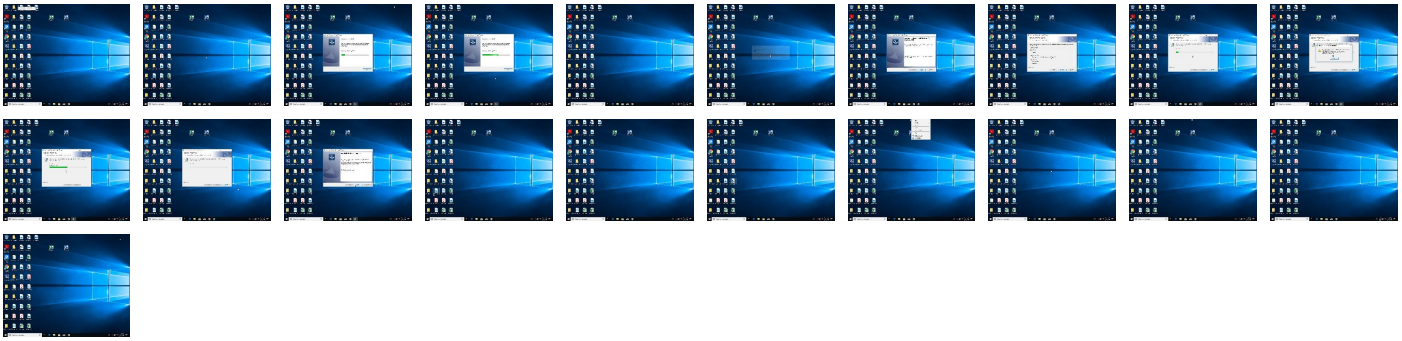
Behavior Graph



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
Setup.exe	0%	Virustotal		Browse
Setup.exe	0%	Metadefender		Browse
Setup.exe	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSI1304.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MSI1304.tmp	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI1304.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.star4live.comi4w	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.star4live.com	0%	Virustotal		Browse
http://www.star4live.com	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

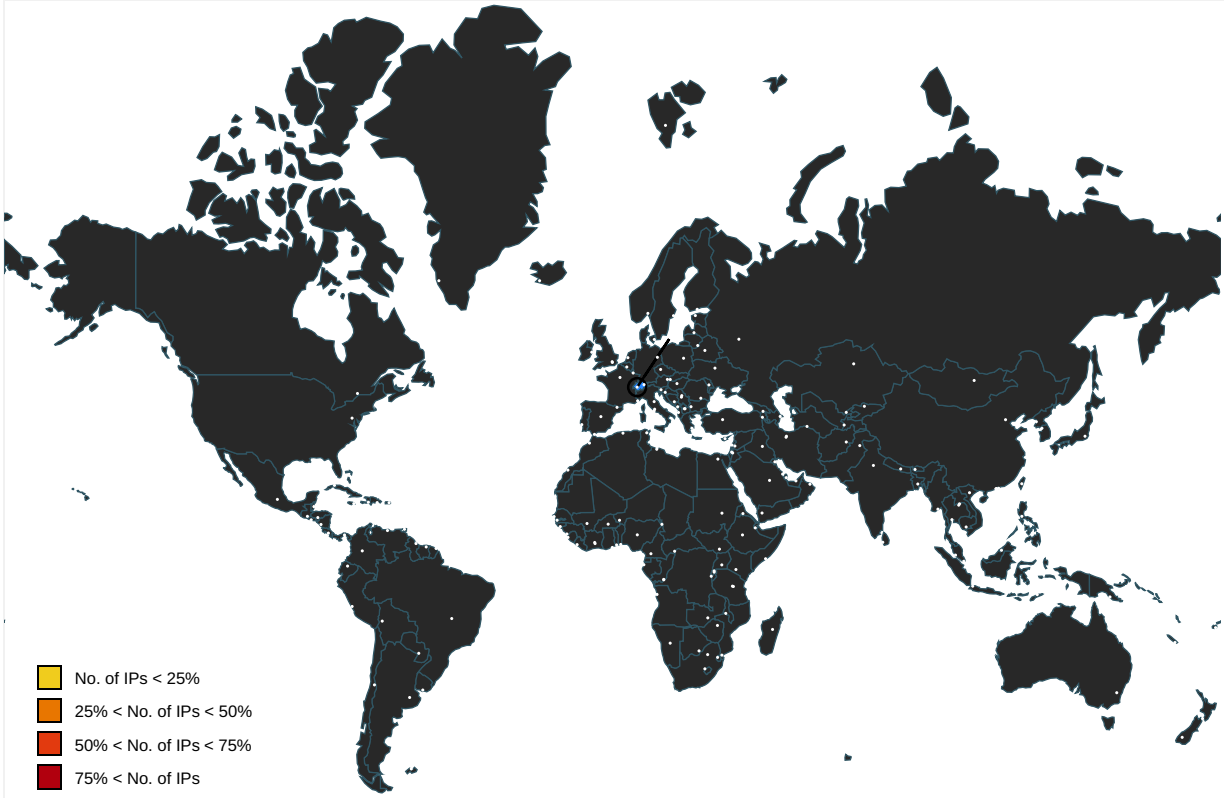
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000001F.00000003.310525588.000001DB23645000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000001F.00000002.310932690.000001DB2363E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000001F.00000002.310932690.000001DB2363E000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000001F.00000003.310023457.000001DB2364B000.00000004.00000001.sdmp	false		high
http://ocsp.thawte.com0	MSI1304.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000001F.00000002.310932690.000001DB2363E000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/enumeration/Enumerate	svchost.exe, 00000019.00000002.466584853.0000029D7B2A0000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000001F.00000003.310525588.000001DB23645000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000001F.00000003.310512253.000001DB23646000.00000004.00000001.sdmp	false		high
http://www.installshield.com/isetup/ProErrorCentral.asp?ErrorCode=%d	Setup.exe	false		high
http://www.star4live.comi4w	msiexec.exe, 00000002.00000003.212346389.00000000033EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000001F.00000002.310932690.000001DB2363E000.00000004.00000001.sdmp, svchost.exe, 0000001F.00000002.310869374.000001DB23613000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000001F.00000002.310942420.000001DB23642000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000001C.00000002.466340191.00000268B822A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000001F.00000003.310023457.000001DB2364B000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000001F.00000003.286601390.000001DB23631000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000001F.00000003.310023457.000001DB2364B000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000001F.00000003.286601390.000001DB23631000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000001F.00000003.310512253.000001DB23646000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 00000019.00000002.470491719.0000029D7C980000.00000002.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000001F.00000002.310942420.000001DB23642000.00000004.00000001.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	MSI1304.tmp.2.dr	false		high
http://https://dynamic.t	svchost.exe, 0000001F.00000002.310997843.000001DB23664000.00000004.00000001.sdmp, svchost.exe, 0000001F.00000002.310942420.000001DB23642000.00000004.00000001.sdmp, svchost.exe, 0000001F.00000003.310518653.000001DB23641000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000001F.00000003.286601390.000001DB23631000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000001F.00000003.310512253.000001DB23646000.00000004.00000001.sdmp	false		high
http://www.flexerasoftware.com0	MSI1304.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://activity.windows.com	svchost.exe, 0000001C.00000002.466340191.00000268B822A000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000001F.00000002.310869374.000001DB23613000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000001F.00000003.309978164.000001DB23660000.00000004.00000001.sdmp	false		high
http://www.star4live.com	Setup.exe, 00000000.00000002.263650863.000000000088A000.00000004.00000020.sdmp, msiexec.exe, 00000002.00000003.254356751.000000000341F000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000001F.00000002.310932690.000001DB2363E000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000001C.00000002.466340191.00000268B822A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000001F.00000003.310023457.000001DB2364B000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358589
Start date:	25.02.2021

Start time:	21:57:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Setup.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:	40
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:	SUS
Classification:	sus24.evad.winEXE@44/20@0/1
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.54.113.53, 104.43.139.144, 52.255.188.83, 104.42.151.234, 40.88.32.150, 13.88.21.125, 52.147.198.201, 51.11.168.160, 184.30.20.56, 8.248.145.254, 67.27.159.254, 8.248.147.254, 8.253.95.121, 8.248.135.254, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Execution Graph export aborted for target msiexec.exe, PID 6708 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • 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
21:58:55	API Interceptor	1x Sleep call for process: CloudHttpWindowPopup.exe modified
21:59:01	API Interceptor	2x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Star4Live\Star4Live_P2P\log\p2plog_20210225-215854.1636	
Process:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpServer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	279
Entropy (8bit):	5.214587635835077
Encrypted:	false
SSDEEP:	6:k3q/Lp/E1f1JHIWCdwmsf+ifbFtoJ52e+q7:QQIvIWlwmsDZA2e+I
MD5:	4E61E2267500AE1D97328057C416826A
SHA1:	B4304C253D27CE2F4E326207425E244E9EA6D9C5
SHA-256:	B680954FC0C1B9D905609014B68DBB16B9BEED694A06631A94A219F9F1BD99ED
SHA-512:	874C4E42FE2A1B08A8721932AAC5C9433357D082232F3331A62870DDE73E516994E92425C5A87B6C33F1A9D6E25E36778B7383FCA952E4503988FEDFDE4AADC8
Malicious:	false
Preview:	Log file created at: 2021/02/25 21:58:54..Running on machine: 632922..Log line format: [IWEF]mmdd hh:mm:ss.uuuuuu threadid file:line] msg..I0225 21:58:54.331068 6012 http_server.cpp:1200] [http_server.cpp:1299] The log path : C:\Program Files (x86)\Star4Live\Star4Live_P2P\log..

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.596673855033803
Encrypted:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SSDEEP:	6:b/k1GaD0JOCEfMuaaD0JOCEfMKQmD31Al/gz2cE0fMbhEZolrRSQ2hyYIIT:bUGaD0JcaaD0JwQQlAg/0bjSQJ
MD5:	87658B0EF52FF2207F7C0E05251F91E8
SHA1:	CDE1D1C3B20E38A13A50EE9EE05F601B9C230C2D
SHA-256:	31C87B83AD51FD46294150292440A95B7DB7E5B41BF9091A5986FA9435E180FB
SHA-512:	DD6EBE1CCC58E54BC78F245E4641AB278E5B282E58769BA944743854E62E8D5623A5A9E52A19876608B9C2D2722FB6456F40A9E26C1604E75182433C5DBC62E
Malicious:	false
Preview:	....E..h..(.....;...y_..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....;...y_.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x7f72b25f, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.0954107310705069
Encrypted:	false
SSDEEP:	12:vG0+01O4bledt/ltKJG0+01O4bledt/ltK:vxhmJCxhmJ
MD5:	5367189EBC18CB591DB7857DDB1C0C81
SHA1:	8BE339EDE8A5E0029E7E3158AA33C4D31E0BCF1C
SHA-256:	39FD24BB07EFC8C77F71EF060AED04DFFED8921FA6906A51F94AFA10D0646316
SHA-512:	496C9E4914F9BA6ACBA10B8F3D2A7F7825FFE5A70728FA6E608D884CE6807189CAA080B2EA0D2C0DF52ECA4FB2C497769B0368D74902C760EC81DD0B5C940A D
Malicious:	false
Preview:	.r._... .....e.f.3...w.....&.....w...;...y_.h.(.....3...w.....B.....@..... ....3...w..... .....h.;...y_k.....%...;...y_..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11126258918616926
Encrypted:	false
SSDEEP:	3:GD/ll7Evkeg/nc0uXl/bJdAtiE2lll:GD/llikeg/nc0At4j2/
MD5:	D79A24EB79A375F59BB4E2921FF76312
SHA1:	95ECB286EFEAEC62BE3E7EADF977CF6F12915783
SHA-256:	0DFE523DBC951B90FAC72CE0D531B5E05C445254A1D0673A1FF997595379F66B
SHA-512:	55152E72E4050A50184658BB5EDFB8F4416F7DDABE01E16B52FF84166CD3B81FC1B92019BE1EB2294D130A669ED822E5ACF56E25026C61FAD28A75EDFC76DC F
Malicious:	false
Preview:	.}`C.....3...w...;...y_.....w.....w.....w....:O.....w.....%...;...y_..... ....

C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Intel;1033
Category:	dropped
Size (bytes):	8905728
Entropy (8bit):	7.93861669664411
Encrypted:	false
SSDEEP:	196608:ebZ7MQgQzFPZhyFs7t8e0ONuly1zyjAHy87Xfb3tsbySjkKnH2HDi:gZQzQXgs7XjZ5yPcfbdgWji
MD5:	7980E58F7A7A619D21360EA557EB6D14
SHA1:	1104563E1CD52A3174DC2C998CFC2C94238F4AC6
SHA-256:	17263403F97F57C23FD20C09D063805A24E083FB23ABFD3E4069B68381F692EF
SHA-512:	AAE3EBE42CDA54CD81D2E12E488DA061A84B9C3A8E0FABA642E63B49ECC2FFFA44111D93F5094E3B7A1E43187FDAAE521AA124BBA2C5F073AA865B9D574E7 0DA
Malicious:	false

C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi	
Preview:	.....>.....8.....6..... ....!..!..".."...#...#...$...$...%...%...&...&...'..'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5 ...5...6.....:......./..... ..!..".."...#...$.....&...&...L...(...)...)...*...*...+...+...,...,...-...-.....%...%...0...0...1...1...2...2...3...3...4...4...5...5...6...6...7...7...>...>...M...M...:...:... <.....=.....=.....?...?...@...@...A...A...B...B...C...C...D...D...E...E...F...F...G...G...H...H...I...I...J...J...O...O...~...~...N...N...d...d...Y...Y...P...P...Q...Q...R...R...S...S...T...T...U...U...V...V...W...W...X...X...[...[...Z...Z...e...e...\...\...]...]...^...^..._...`...`...a...a...b...b...c...c...d...d...g...g...f.....f.....h...h...i...i...j...j...k...k...l...l...m...m...n...n...o...o...p...p...q...q...r...r...s...s...t...t...u...u...v...v...w...w...x...x...y...y...z...z...

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11000108893909519
Encrypted:	false
SSDEEP:	12:264KzXm/Ey6q99953jHq3qQ10nMCldimE8eawHjcVtEv:264vl680LyMCldzE9BHjcVtE
MD5:	AE43C15CDF4DCEAA79848D82AC05CEBE
SHA1:	488368599190E000EF11016658D1B54E6C445969
SHA-256:	01B20327D30557A171734057B9A7A4C24BD36745897CB73424019D9859EF6FFF
SHA-512:	3FD6722160EFC0183B459B37E3393CB43F6364E0359398F8A1719096259B8F89B79B0443FF1D72DF3BD1E21984AA65F4F063F7265CF3A89F4F26462B79748C6F
Malicious:	false
Preview:	.....P.....<.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....g..-..... .....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.P..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11247914257248325
Encrypted:	false
SSDEEP:	12:PyMzXm/Ey6q99953jz1miM3qQ10nMCldimE8eawHza1miINf:PYl68Z1tMLyMCldzE9BHza1tlV
MD5:	006591B85AEE4C755D9D0FCFD4E6960B
SHA1:	4721917B747140CDFA4D60AD8C492D290D1FCEB8
SHA-256:	A20EDDF428C8AD104073D97ED8C8117CE4EEFC6D7193EDA9A2E593A1D1FC01B5
SHA-512:	2D142EE08627A2A8B0C2FFE9F7F46ECB03E11E9A244B8240E508B11CB4601585300F54DE118DC4AC0D3DE855DDDFDFF8F72417D5EF29FCE0003BE6F568C0163
Malicious:	false
Preview:	.....P.....k.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....g..-..... .....F.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.P.....!..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11218613222979573
Encrypted:	false
SSDEEP:	12:LzXm/Ey6q99953jV1mK2P3qQ10nMCldimE8eawHza1mKwf:2l68T1iPLyMCldzE9BHza1U
MD5:	BEF68CE3004440C64AA8113734E2063E
SHA1:	D71E5548E0287D1421524ADD354C455901047436
SHA-256:	E159E42261B950E66A7B714848248B622A88E3B062B354808BA02FB52607ABA6
SHA-512:	5C8E0D1CCBD8DFE46C47F09A9EAA95BDFC045E7D147F2B4924A5F827469A9D110B0E55D5FBEE9E844964398EBF2B1B72424334F9E84969D9F2E7CA655A93F40C
Malicious:	false
Preview:	.....P.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....g..-..... .....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.P.....z..... ....

C:\Users\user\AppData\Local\Temp\MSI1304.tmp	
Process:	C:\Windows\SysWOW64\msiexec.exe

C:\Users\user\AppData\Local\Temp\MSI1304.tmp	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	154960
Entropy (8bit):	6.025909749036716
Encrypted:	false
SSDEEP:	3072:6x1vl8koSXMXm3o1dSjr+MEwW1nd0DOT6Tt:6TvioSXDof8rCp6Tt
MD5:	778D0941FB9B969AB90B81C9B91086D7
SHA1:	02B755BE2046F5B34F5884AF9137ED014023E2E1
SHA-256:	3A2EB487237D36B6DA8CC21EB39AFDB890A84BF2E29FADF3182E44B1EF114FB8
SHA-512:	E6B384B3C958D597B9D842E50627EE5EA52DFFC5776A876E2BED3027C242A7184248E734C7204E56DCC325EFBA24D4F14A1B8F0DF073190B51DB21E06AA2C018
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....[.....[.....[.....nF....nV.....x.....R. .....Rich.....PE..L.....pR.....!.....H.....`.....E...\.....@.....D..P....P..(.....@.. .....`.....text....G.....H..... ..`.rdata.....`.....L.....@..@.data...t2.....@....rsrc.....@.....@..@.reloc..<J...P...L..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\MSI715f3.LOG	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	748
Entropy (8bit):	3.722960589618841
Encrypted:	false
SSDEEP:	12:Qw5U3zfU1XQ9kvlCQkpdZLl2lLBrL6AFYelmSTMlWlKUFlCKgPH:QkU3YK+KpbRKVrLpFjmYkWQUF+H
MD5:	E8FB56C24773DFF2E1FBB38C5D657AA9
SHA1:	EEEAF27F51C4350F9AB5DFF463CDCC1BFDBDF1EE
SHA-256:	104F3794C8A2F57356FBCF753A67A4A78904A2E87A2399629054F843A44E6E03
SHA-512:	1B9BA6A29E3ED2B02C7EBBCEB22C4293356527C3AE93E51712BA2C49C69DB1AA15E3694A0D8821A4E8F0C40C56D8E0D17FDC7F3ADFAEA6CFD496899F8EF8E2B0
Malicious:	false
Preview:	..E.r.r.o.r. .1.9.3.5... .A.n. .e.r.r.o.r. .o.c.c.u.r.r.e.d. .d.u.r.i.n.g. .t.h.e. .i.n.s.t.a.l.l.a.t.i.o.n. .o.f. .a.s.s.e.m.b.l.y. .c.o.m.p.o.n.e.n.t. .{.B.7.0.8.E.B.7.2.-.A.A.8.2.-.3.E.B.7.-.8.B.B.0.-.D.8.4.5.B.A.3.5.C.9.3.D.}... .H.R.E.S.U.L.T.:. .0.x.8.0.0.7.0.4.2.2... .a.s.s.e.m.b.l.y. .i.n.t.e.r.f.a.c.e.:. .I.A.s.s.e.m.b.l.y.C.a.c.h.e.I.t.e.m.,. .f.u.n.c.t.i.o.n.:. .C.o.m.m.i.t.,. .a.s.s.e.m.b.l.y. .n.a.m.e.:. .M.i.c.r.o.s.o.f.t...V.C.9.0...C.R.T.,.v.e.r.s.i.o.n.=.".9...0...2.1.0.2.2...8.".,.p.u.b.l.i.c.K.e.y.T.o.k.e.n.=.".1.f.c.8.b.3.b.9.a.1.e.1.8.e.3.b.".,.p.r.o.c.e.s.s.o.r.A.r.c.h.i.t.e.c.t.u.r.e.=.".x.8.6.".,.t.y.p.e.=.".w.i.n.3.2.".....=.=.=. .L.o.g.g.i.n.g. .s.t.o.p.p.e.d.:. .2./.2.5./.2.0.2.1. . .2.1.:.5.8.:.5.9. .=.=.=.....

C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	22492
Entropy (8bit):	3.484893836872466
Encrypted:	false
SSDEEP:	384:CTmyuV//BiTbh/G4AwC2WrP2DBWa/Oa0Mhs+XVgv:CT6V//BiXh/z/lWr0aa0Mhs+XVgv
MD5:	BE345D0260AE12C5F2F337B17E07C217
SHA1:	0976BA0982FE34F1C35A0974F6178E15C238ED7B
SHA-256:	E994689A13B9448C074F9B471EDEEC9B524890A0D82925E98AB90B658016D8F3
SHA-512:	77040DBEE29BE6B136A83B9E444D8B4F71FF739F7157E451778FB4FCCB939A67FF881A70483DE16BCB6AE1FEA64A89E00711A33EC26F4D3EEA8E16C9E9553EF
Malicious:	false
Preview:	..[.0.x.0.4.0.9.].....1.1.0.0.=.S.e.t.u.p. .I.n.i.t.i.a.l.i.z.a.t.i.o.n. .E.r.r.o.r.....1.1.0.1.=.%.s.....1.1.0.2.=.%.1. .S.e.t.u.p. .i.s. .p.r.e.p.a.r.i.n.g. .t.h.e. .%.2.,. .w.h.i.c.h. .w.i.l.l. .g.u.i.d.e. .y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m. .s.e.t.u.p. .p.r.o.c.e.s.s... . .P.l.e.a.s.e. .w.a.i.t.....1.1.0.3.=.C.h.e.c.k.i.n.g. .O.p.e.r.a.t.i.n.g. .S.y.s.t.e.m. .V.e.r.s.i.o.n.....1.1.0.4.=.C.h.e.c.k.i.n.g. .W.i.n.d.o.w.s.(.R.). .I.n.s.t.a.l.l.e.r. .V.e.r.s.i.o.n.....1.1.0.5.=.C.o.n.f.i.g.u.r.i.n.g. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r.....1.1.0.6.=.C.o.n.f.i.g.u.r.i.n.g. .%.s.....1.1.0.7.=.S.e.t.u.p. .h.a.s. .c.o.m.p.l.e.t.e.d. .c.o.n.f.i.g.u.r.i.n.g. .t.h.e. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r. .o.n. .y.o.u.r. .s.y.s.t.e.m... .T.h.e. .s.y.s.t.e.m. .n.e.e.d.s. .t.o. .b.e. .r.e.s.t.a.r.t.e.d. .i.n. .o.r.d.e.r. .t.o. .c.o.n.t.i.n.u.e. .w.i.t.h. .t.h.e. .i.n.s.t.a.l.l.a.t.i.o.n... .P.l.e.a.s.e. .c.l.i.c.k. .R.e.s.t.a.r.t. .t.o. .r.e.b.o.o.t. .t.h.e. .s.y.s.t.e.m.....1.1.0.8.

C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	5174
Entropy (8bit):	3.705975630008245
Encrypted:	false

C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	
SSDEEP:	96:rEhkMaE1QJgQxH1meON/XsEbFWaEPRhS+gWPQPgWRGTwQbPrvnp6kY05w7tCYOvY:YhcbMFcuQaEZhdxoIWRGcQbPr/p00509
MD5:	DCBA353F2B7EADE8FE50D59107AAFCF2
SHA1:	93260BC97E343BCAB65179A8E84D014B8F2B839D
SHA-256:	46342A1CEE706944285ABAA51C1E02C0BE9AF43F48ACFD97AC2AFC0B10C31B45
SHA-512:	82D99683CA4456990731218D5C521D866C0AAC63D88F9689DAFC16870C32B03C808A74017A3120393357B31804E42242F746A34E94F5473DF602B717BEDFF5A2
Malicious:	false
Preview:	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=.....S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r.i.p.t.D.r.i.v.e.n.=.0.....S.c.r.i.p.t.V.e.r.=.1...0...0...1.....D.o.t.N.e.t.O.p.t.i.o.n.a.l.l.n.s.t.a.l.l.l.f.S.i.l.e.n.t.=.N.....O.n.U.p.g.r.a.d.e.=.0.....P.r.o.d.u.c.t.=.S.t.a.r.4.L.i.v.e._.P.2.P.....P.a.c.k.a.g.e.N.a.m.e.=.S.t.a.r.4.L.i.v.e._.P.2.P...m.s.i.....E.n.a.b.l.e.L.a.n.g.D.l.g.=.Y.....L.o.g.R.e.s.u.l.t.s.=.N.....D.o.M.a.i.n.t.e.n.a.n.c.e.=.N.....P.r.o.d.u.c.t.C.o.d.e.=.{.1.8.6.B.E.9.3.2.-.E.2.8.A.-.4.F.4.7.-.9.6.0.F.-.A.C.1.F.1.2.3.C.1.7.0.3.}.....P.r.o.d.u.c.t.V.e.r.s.i.o.n.=.1...2.0...0.0.0.1.....L.a.u.n.c.h.e.r.N.a.m.e.=.s.e.t.u.p...e.x.e.....P.a.c.k.a.g.e.C.o.d.e.=.{.8.7.7.F.9.B.E.8.-.C.6.E.2.-.4.6.2.D.-.9.A.9.6.-.0.9.E.4.2.3.9.0.D.0.0.2.}.....[.L.a.n.g.u.a.g.e.s.].....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.

C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Star4Live_P2P.msi	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Intel;1033
Category:	dropped
Size (bytes):	8905728
Entropy (8bit):	7.93861669664411
Encrypted:	false
SSDEEP:	196608:ebZ7MQgQzFPZhyFs7t8e0ONuly1zyjAHy87Xfb3tsbySjkKnH2HDi:gZQzQXgs7XjZ5yPcfbdgWji
MD5:	7980E58F7A7A619D21360EA557EB6D14
SHA1:	1104563E1CD52A3174DC2C998CFC2C94238F4AC6
SHA-256:	17263403F97F57C23FD20C09D063805A24E083FB23ABFD3E4069B68381F692EF
SHA-512:	AAE3EBE42CDA54CD81D2E12E488DA061A84B9C3A8E0FABA642E63B49ECC2FFFA44111D93F5094E3B7A1E43187FDAAE521AA124BBA2C5F073AA865B9D574E70DA
Malicious:	false
Preview:	.....>.....8.....6..... ....!...!..."..."...#...#...$...$...%...%...&...&...'...'...(...(...)...)...*...*...+...+...,...,...-...-...../.../...0...0...1...1...2...2...3...3...4...4...5...5...6.....:...../..... ...!..."...#...$.....&...L...(...)...*...+...,...-.....%...0...1...2...3...4...5...6...7...>...M...:... <.....=.....?...@...A...B...C...D...E...F...G...H...I...J...O...~...N...d...Y...P...Q...R...S...T...U...V...W...X...[...Z...e...\...]...^..._...`...a...b...c...d...g...f.....h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1916
Entropy (8bit):	3.712189476309667
Encrypted:	false
SSDEEP:	24:Q+wLWLfLWLfLTQjLDQqLTQjLDQSQjLDQ2:rwLWLfLWLfLTQjLDQqLTQjLDQSQjLDQ2
MD5:	077E0E8202E2636BE1A5AB5594F7FDA3
SHA1:	8F32ED8E55CCB85DE61C7B7F1D4F50B2F7C286BA
SHA-256:	8540397DE3619048525551C3CB58987231604A7A870F274181DA2A0DA6302112
SHA-512:	26F07CC6E3D0DB9E12D8448BDE1F6EAAFD019D8ABCA504B89D6E3AE8A7695393175EE5AF7836D1690317F90C50154675E93810529A8EB2B81379F9B1690AF9A
Malicious:	false
Preview:	..[.F.i.l.e.s.].....S.e.t.u.p...I.N.I.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.{.4.2.9.B.5.C.B.3.-.3.3.9.E.-.4.8.3.B.-.9.0.3.2.-.C.B.0.D.A.1.4.F.2.F.9.A.}.\.S.e.t.u.p...I.N.I.....[.F.i.l.e.s.].....0.x.0.4.0.9...i.n.i.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.{.4.2.9.B.5.C.B.3.-.3.3.9.E.-.4.8.3.B.-.9.0.3.2.-.C.B.0.D.A.1.4.F.2.F.9.A.}.\.0.x.0.4.0.9...i.n.i.....S.e.t.u.p...I.N.I.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.{.4.2.9.B.5.C.B.3.-.3.3.9.E.-.4.8.3.B.-.9.0.3.2.-.C.B.0.D.A.1.4.F.2.F.9.A.}.\.S.e.t.u.p...I.N.I.....[.F.i.l.e.s.].....0.x.0.4.0.9...i.n.i.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.{.4.2.9.B.5.C.B.3.-.3.3.9.E.-.4.8.3.B.-.9.0.3.2.-.C.B.0.D.A.1.4.F.2.F.9.A.}.\.0.x.0.4.0.9...i.n.i.....S.e.t.u.p...I.N.I.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.{.4.2.9.B.5.C.B.3.-.3.3.9.E.-.4.8.3.B.-.9.0.3.2.-.C.B.0.D.A.1.4.F.2.F.9.A.}.\.S.e.t.u.p...I.

C:\Users\user\AppData\Local\Temp\~F49E.tmp	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	5174
Entropy (8bit):	3.705975630008245
Encrypted:	false
SSDEEP:	96:rEhkMaE1QJgQxH1meON/XsEbFWaEPRhS+gWPQPgWRGTwQbPrvnp6kY05w7tCYOvY:YhcbMFcuQaEZhdxoIWRGcQbPr/p00509
MD5:	DCBA353F2B7EADE8FE50D59107AAFCF2
SHA1:	93260BC97E343BCAB65179A8E84D014B8F2B839D
SHA-256:	46342A1CEE706944285ABAA51C1E02C0BE9AF43F48ACFD97AC2AFC0B10C31B45
SHA-512:	82D99683CA4456990731218D5C521D866C0AAC63D88F9689DAFC16870C32B03C808A74017A3120393357B31804E42242F746A34E94F5473DF602B717BEDFF5A2
Malicious:	false

C:\Users\user\AppData\Local\Temp\~F49E.tmp	
Preview:	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=.....S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r.i.p.t.D.r.i.v.e.n.=.0.....S.c.r.i.p.t.V.e.r.=.1...0...0...1.....D.o.t.N.e.t.O.p.t.i.o.n.a.l.l.n.s.t.a.l.l.f.S.i.l.e.n.t.=.N.....O.n.U.p.g.r.a.d.e.=.0.....P.r.o.d.u.c.t.=.S.t.a.r.4.L.i.v.e._.P.2.P.....P.a.c.k.a.g.e.N.a.m.e.=.S.t.a.r.4.L.i.v.e._.P.2.P...m.s.i.....E.n.a.b.l.e.L.a.n.g.D.l.g.=.Y.....L.o.g.R.e.s.u.l.t.s.=.N.....D.o.M.a.i.n.t.e.n.a.n.c.e.=.N.....P.r.o.d.u.c.t.C.o.d.e.=.{.1.8.6.B.E.9.3.2.-.E.2.8.A.-.4.F.4.7.-.9.6.0.F.-.A.C.1.F.1.2.3.C.1.7.0.3.}.....P.r.o.d.u.c.t.V.e.r.s.i.o.n.=.1...2.0...0.0.0.1.....L.a.u.n.c.h.e.r.N.a.m.e.=.s.e.t.u.p...e.x.e.....P.a.c.k.a.g.e.C.o.d.e.=.{.8.7.7.F.9.B.E.8.-.C.6.E.2.-.4.6.2.D.-.9.A.9.6.-.0.9.E.4.2.3.9.0.D.0.0.2.}.....[.L.a.n.g.u.a.g.e.s.].....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.

C:\Users\user\AppData\Local\Temp\~F4CE.tmp	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	5174
Entropy (8bit):	3.705975630008245
Encrypted:	false
SSDEEP:	96:rEhkMaE1QJgQxH1meON/XsEbFWaEPRhS+gWPQPgWRGTwQbPrvnp6kY05w7tCYOvY:YhcbMFcuQaEZhdxoIWRGcQbPr/p00509
MD5:	DCBA353F2B7EADE8FE50D59107AAFCF2
SHA1:	93260BC97E343BCAB65179A8E84D014B8F2B839D
SHA-256:	46342A1CEE706944285ABAA51C1E02C0BE9AF43F48ACFD97AC2AFC0B10C31B45
SHA-512:	82D99683CA4456990731218D5C521D866C0AAC63D88F9689DAFC16870C32B03C808A74017A3120393357B31804E42242F746A34E94F5473DF602B717BEDFF5A2
Malicious:	false
Preview:	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=.....S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r.i.p.t.D.r.i.v.e.n.=.0.....S.c.r.i.p.t.V.e.r.=.1...0...0...1.....D.o.t.N.e.t.O.p.t.i.o.n.a.l.l.n.s.t.a.l.l.f.S.i.l.e.n.t.=.N.....O.n.U.p.g.r.a.d.e.=.0.....P.r.o.d.u.c.t.=.S.t.a.r.4.L.i.v.e._.P.2.P.....P.a.c.k.a.g.e.N.a.m.e.=.S.t.a.r.4.L.i.v.e._.P.2.P...m.s.i.....E.n.a.b.l.e.L.a.n.g.D.l.g.=.Y.....L.o.g.R.e.s.u.l.t.s.=.N.....D.o.M.a.i.n.t.e.n.a.n.c.e.=.N.....P.r.o.d.u.c.t.C.o.d.e.=.{.1.8.6.B.E.9.3.2.-.E.2.8.A.-.4.F.4.7.-.9.6.0.F.-.A.C.1.F.1.2.3.C.1.7.0.3.}.....P.r.o.d.u.c.t.V.e.r.s.i.o.n.=.1...2.0...0.0.0.1.....L.a.u.n.c.h.e.r.N.a.m.e.=.s.e.t.u.p...e.x.e.....P.a.c.k.a.g.e.C.o.d.e.=.{.8.7.7.F.9.B.E.8.-.C.6.E.2.-.4.6.2.D.-.9.A.9.6.-.0.9.E.4.2.3.9.0.D.0.0.2.}.....[.L.a.n.g.u.a.g.e.s.].....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.

C:\Users\user\AppData\Local\Temp\~FC32.tmp	
Process:	C:\Users\user\Desktop\Setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	5174
Entropy (8bit):	3.705975630008245
Encrypted:	false
SSDEEP:	96:rEhkMaE1QJgQxH1meON/XsEbFWaEPRhS+gWPQPgWRGTwQbPrvnp6kY05w7tCYOvY:YhcbMFcuQaEZhdxoIWRGcQbPr/p00509
MD5:	DCBA353F2B7EADE8FE50D59107AAFCF2
SHA1:	93260BC97E343BCAB65179A8E84D014B8F2B839D
SHA-256:	46342A1CEE706944285ABAA51C1E02C0BE9AF43F48ACFD97AC2AFC0B10C31B45
SHA-512:	82D99683CA4456990731218D5C521D866C0AAC63D88F9689DAFC16870C32B03C808A74017A3120393357B31804E42242F746A34E94F5473DF602B717BEDFF5A2
Malicious:	false
Preview:	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=.....S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r.i.p.t.D.r.i.v.e.n.=.0.....S.c.r.i.p.t.V.e.r.=.1...0...0...1.....D.o.t.N.e.t.O.p.t.i.o.n.a.l.l.n.s.t.a.l.l.f.S.i.l.e.n.t.=.N.....O.n.U.p.g.r.a.d.e.=.0.....P.r.o.d.u.c.t.=.S.t.a.r.4.L.i.v.e._.P.2.P.....P.a.c.k.a.g.e.N.a.m.e.=.S.t.a.r.4.L.i.v.e._.P.2.P...m.s.i.....E.n.a.b.l.e.L.a.n.g.D.l.g.=.Y.....L.o.g.R.e.s.u.l.t.s.=.N.....D.o.M.a.i.n.t.e.n.a.n.c.e.=.N.....P.r.o.d.u.c.t.C.o.d.e.=.{.1.8.6.B.E.9.3.2.-.E.2.8.A.-.4.F.4.7.-.9.6.0.F.-.A.C.1.F.1.2.3.C.1.7.0.3.}.....P.r.o.d.u.c.t.V.e.r.s.i.o.n.=.1...2.0...0.0.0.1.....L.a.u.n.c.h.e.r.N.a.m.e.=.s.e.t.u.p...e.x.e.....P.a.c.k.a.g.e.C.o.d.e.=.{.8.7.7.F.9.B.E.8.-.C.6.E.2.-.4.6.2.D.-.9.A.9.6.-.0.9.E.4.2.3.9.0.D.0.0.2.}.....[.L.a.n.g.u.a.g.e.s.].....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

\Device\ConDrv	
Process:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWindowPopup.exe
File Type:	ASCII text, with CRLF line terminators

\Device\ConDrv	
Category:	dropped
Size (bytes):	21
Entropy (8bit):	3.5944656369614525
Encrypted:	false
SSDEEP:	3:6zXx5xvn:O5xvn
MD5:	102A76544A6788499EAE34CFC9CE5EAD
SHA1:	91522965860BC7D33334C6AC8D28314A0CA45F5F
SHA-256:	73B22483CA5FDA42A40744D2AADA12D852DC3C1C0D27DA2CE99400FC0F99E15F
SHA-512:	CC189637A68725AF611292C834BFBAED954724111C174AF9C5BAB9006C5D7FDB9FB5F18F2A241892308098D0C1398A5CA650B9C2611FB0C8B391CB4A1F653CD
Malicious:	false
Preview:	connect error:10061..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9512498814931805
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • InstallShield setup (43055/19) 0.43% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Setup.exe
File size:	9610518
MD5:	7b5d30bd9b7cdcca79e189aaaf5707fa
SHA1:	45fe889c3660be692ba30bb6bcdc2b51380c214e
SHA256:	a6385ebfc0c6e766e9f068ad348a53e39a18875da5e3759 428633984c0b075aa
SHA512:	65ea09cb65ddcc505ccf35bfacc50636775419b4ecd9db9 69bd1cbfb4241ac881e3bc3d0c4d286b0e107cc447a2f74 d9e574b466faaf7e83fdaf805156622c38
SSDEEP:	196608:VaVciYErjGFUbetSBd6maXuNIeHnbrMhrcXG5 RVlixlXF67EPz3X:V+5rjGFUbesN3IeMKGJlixlKurX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.|GB./ GB./GB./N:./LB./N:./]B./N:./.B./`../DB./Y../DB./`../RB./GB. /#C./N:./3B./Y../FB./N:./FB./RichGB./.....PE..L..

File Icon

Icon Hash:	b6c93933cc71278a

Static PE Info

General

Entrypoint:	0x46b0fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5270ABA2 [Wed Oct 30 06:48:02 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0

General	
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	8716dfcb53e9237687620dc5ebbd5d82

Entrypoint Preview

Instruction
call 00007F72A8772A13h
jmp 00007F72A876011Eh
test eax, eax
je 00007F72A87602AFh
xor ecx, ecx
test eax, eax
setnle cl
lea ecx, dword ptr [ecx+ecx-01h]
mov eax, ecx
ret
movzx eax, byte ptr [eax]
movzx ecx, byte ptr [ecx]
sub eax, ecx
je 00007F72A87602AFh
xor ecx, ecx
test eax, eax
setnle cl
lea ecx, dword ptr [ecx+ecx-01h]
mov eax, ecx
ret
mov ax, word ptr [esi]
cmp ax, word ptr [ecx]
je 00007F72A87602D7h
movzx edx, byte ptr [ecx]
movzx eax, al
sub eax, edx
je 00007F72A87602B3h
xor edx, edx
test eax, eax
setnle dl
lea edx, dword ptr [edx+edx-01h]
mov eax, edx
test eax, eax
jne 00007F72A87602BEh
movzx eax, byte ptr [esi+01h]
movzx ecx, byte ptr [ecx+01h]
sub eax, ecx
je 00007F72A87602B2h
xor ecx, ecx
test eax, eax
setnle cl
lea ecx, dword ptr [ecx+ecx-01h]
mov eax, ecx
ret
xor eax, eax
ret
mov eax, dword ptr [esi]
cmp eax, dword ptr [ecx]
je 00007F72A8760311h
movzx edx, byte ptr [ecx]
movzx eax, al
sub eax, edx
je 00007F72A87602B3h
xor edx, edx
test eax, eax
setnle dl
lea edx, dword ptr [edx+edx-01h]

Instruction
mov eax, edx
test eax, eax
jne 00007F72A87602F8h
movzx eax, byte ptr [esi+01h]
movzx edx, byte ptr [ecx+01h]
sub eax, edx
je 00007F72A87602B3h
xor edx, edx
test eax, eax
setnle dl
lea edx, dword ptr [edx+edx-01h]
mov eax, edx
test eax, eax
jne 00007F72A87602DBh
movzx eax, byte ptr [esi+02h]
movzx edx, byte ptr [ecx+02h]
sub eax, edx
je 00007F72A87602B3h
xor edx, edx
test eax, eax
setnle dl
lea edx, dword ptr [edx+edx+00h]

Rich Headers

Programming Language:	• [ASM] VS2008 SP1 build 30729 • [C] VS2008 SP1 build 30729 • [C] VS2005 build 50727 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [C++] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd7984	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe3000	0x4df28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb0660	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc1d38	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb0000	0x570	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xd7860	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xaeb3d	0xaec00	False	0.505110537375	data	6.58906831396	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb0000	0x2967c	0x29800	False	0.383930252259	data	4.89785688972	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xda000	0x8828	0x2800	False	0.30625	data	4.54037080678	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe3000	0x4df28	0x4e000	False	0.377288035857	data	6.57455992385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
GIF	0xe3e54	0x5731	GIF image data, version 89a, 175 x 312		
GIF	0xe9588	0x6592	GIF image data, version 89a, 175 x 312	English	United States
RT_BITMAP	0xefb1c	0x14220	data		
RT_BITMAP	0x103d3c	0x1b5c	data		
RT_BITMAP	0x105898	0x38e4	data		
RT_BITMAP	0x10917c	0x1238	data		
RT_BITMAP	0x10a3b4	0x6588	data		
RT_BITMAP	0x11093c	0x11f88	data		
RT_ICON	0x1228c4	0x668	data		
RT_ICON	0x122f2c	0x2e8	data		
RT_ICON	0x123214	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x12333c	0xea8	data		
RT_ICON	0x1241e4	0x8a8	data		
RT_ICON	0x124a8c	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x124ff4	0x25a8	data		
RT_ICON	0x12759c	0x10a8	data		
RT_ICON	0x128644	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x128aac	0x2e8	data		
RT_ICON	0x128d94	0x2e8	data		
RT_DIALOG	0x12907c	0x1ee	data		
RT_DIALOG	0x12926c	0x286	data		
RT_DIALOG	0x1294f4	0x2d0	data		
RT_DIALOG	0x1297c4	0x54	data		
RT_DIALOG	0x129818	0x42	data		
RT_DIALOG	0x12985c	0xe6	data		
RT_DIALOG	0x129944	0x124	data		
RT_DIALOG	0x129a68	0xd6	data		
RT_DIALOG	0x129b40	0x266	data		
RT_DIALOG	0x129da8	0x3d8	data		
RT_DIALOG	0x12a180	0x172	data		
RT_DIALOG	0x12a2f4	0x20c	data		
RT_DIALOG	0x12a500	0x1ea	data		
RT_DIALOG	0x12a6ec	0x212	data		
RT_DIALOG	0x12a900	0x7c	data		
RT_DIALOG	0x12a97c	0x3cc	data		
RT_DIALOG	0x12ad48	0x158	data		
RT_DIALOG	0x12aea0	0x1ea	data		
RT_DIALOG	0x12b08c	0x116	data		
RT_DIALOG	0x12b1a4	0xee	data		
RT_DIALOG	0x12b294	0x1d4	data		
RT_DIALOG	0x12b468	0x1ec	data		
RT_DIALOG	0x12b654	0x2b8	data		
RT_STRING	0x12b90c	0x160	data	English	United States
RT_STRING	0x12ba6c	0x23e	data	English	United States
RT_STRING	0x12bcac	0x378	data	English	United States
RT_STRING	0x12c024	0x252	data	English	United States
RT_STRING	0x12c278	0x1f4	data	English	United States
RT_STRING	0x12c46c	0x66c	data	English	United States
RT_STRING	0x12cad8	0x366	data	English	United States
RT_STRING	0x12ce40	0x27e	data	English	United States
RT_STRING	0x12d0c0	0x518	data	English	United States
RT_STRING	0x12d5d8	0x882	data	English	United States
RT_STRING	0x12de5c	0x23e	data	English	United States
RT_STRING	0x12e09c	0x3ba	data	English	United States
RT_STRING	0x12e458	0x12c	data	English	United States
RT_STRING	0x12e584	0x4a	data	English	United States
RT_STRING	0x12e5d0	0xda	data	English	United States
RT_STRING	0x12e6ac	0x110	data	English	United States
RT_STRING	0x12e7bc	0x20a	data	English	United States
RT_STRING	0x12e9c8	0xba	data	English	United States
RT_STRING	0x12ea84	0xa8	data	English	United States
RT_STRING	0x12eb2c	0x12a	data	English	United States
RT_STRING	0x12ec58	0x422	data	English	United States
RT_STRING	0x12f07c	0x5c2	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x12f640	0x40	data	English	United States
RT_STRING	0x12f680	0xcaa	data	English	United States
RT_STRING	0x13032c	0x284	data	English	United States
RT_GROUP_ICON	0x1305b0	0x84	data		
RT_GROUP_ICON	0x130634	0x14	data		
RT_GROUP_ICON	0x130648	0x14	data		
RT_VERSION	0x13065c	0x41c	data		
RT_MANIFEST	0x130a78	0x4af	XML 1.0 document, ASCII text, with CRLF line terminators		

Imports

DLL	Import
VERSION.dll	VerQueryValueW, GetFileVersionInfoSizeW, GetFileVersionInfoW
COMCTL32.dll	
KERNEL32.dll	SizeofResource, LoadResource, FindResourceW, GlobalUnlock, GlobalLock, GlobalFree, GetTickCount, GetExitCodeThread, CreateThread, CopyFileW, InterlockedIncrement, GetVersionExW, CompareStringA, CompareStringW, CreateEventW, InterlockedDecrement, QueryPerformanceFrequency, lstrcatW, GetTempFileNameW, LoadLibraryW, FreeLibrary, GetProcAddress, GetSystemDefaultLangID, GetUserDefaultLangID, lstrcmpW, lstrcmpiW, VerLanguageNameW, FindClose, FindNextFileW, CompareFileTime, FindFirstFileW, MoveFileW, GetPrivateProfileStringW, CreateDirectoryW, SetFileAttributesW, GetSystemTimeAsFileTime, LocalFree, FormatMessageW, GetSystemInfo, MulDiv, RaiseException, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, LoadLibraryExW, GetModuleHandleW, GetVersion, GetLocalTime, IsValidLocale, GetFileAttributesW, GetCommandLineW, lstrcpyA, VirtualQuery, IsBadReadPtr, FlushFileBuffers, SetEndOfFile, GetDriveTypeW, GetLocaleInfoW, GetCurrentThread, GetDiskFreeSpaceW, GetExitCodeProcess, LocalAlloc, InterlockedExchange, GlobalAlloc, SetStdHandle, GetTimeZoneInformation, GetConsoleMode, GetConsoleCP, LCMapStringA, InitializeCriticalSectionAndSpinCount, SetConsoleCtrlHandler, SetThreadContext, GetStringTypeA, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, GetDateFormatA, GetTimeFormatA, GetStartupInfoA, GetFileType, SetHandleCount, GetEnvironmentStringsW, FreeEnvironmentStringsW, HeapDestroy, HeapCreate, HeapReAlloc, VirtualAlloc, VirtualFree, FatalAppExitA, GetModuleHandleA, LCMapStringW, IsValidCodePage, GetOEMCP, GetACP, GetCPInfo, HeapSize, GetCurrentThreadId, TlsFree, TlsSetValue, TlsAlloc, TlsGetValue, GetModuleFileNameA, GetStdHandle, GetStartupInfoW, IsDebuggerPresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter, RtlUnwind, lstrcpynA, lstrcmpA, SearchPathW, VirtualProtect, lstrlenW, SystemTimeToFileTime, QueryPerformanceCounter, SetEvent, ResetEvent, GetCurrentProcessId, GetEnvironmentVariableW, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, GetDateFormatW, GetTimeFormatW, GetCurrentDirectoryW, FindResourceExW, GetFileTime, SetFileTime, LockResource, ExpandEnvironmentStringsW, GetTempPathW, SetErrorMode, GetWindowsDirectoryW, lstrcpyW, GetSystemDirectoryW, SetCurrentDirectoryW, CreateProcessW, WaitForSingleObject, DeleteFileW, RemoveDirectoryW, Sleep, ExitProcess, GetCurrentProcess, DuplicateHandle, TerminateProcess, MoveFileExW, GetThreadContext, VirtualProtectEx, WriteProcessMemory, GetModuleFileNameW, FlushInstructionCache, lstrcpynW, GetProcessHeap, HeapAlloc, HeapFree, WriteFile, ReadFile, SetFilePointer, MultiByteToWideChar, WideCharToMultiByte, CreateFileW, GetFileSize, CreateFileMappingW, MapViewOfFile, UnmapViewOfFile, CloseHandle, lstrlenA, GetLastError, SetLastError, GetStringTypeW, ResumeThread, SetEnvironmentVariableA, OpenProcess, GetProcessTimes, CreateFileA, WriteConsoleW, LoadLibraryA, WriteConsoleA, GetConsoleOutputCP
USER32.dll	ExitWindowsEx, CharUpperW, wvsprintfW, SendDlgItemMessageW, CharPrevW, LoadImageW, CreateDialogParamW, MoveWindow, SetCursor, GetDlgItemTextW, GetWindow, SetFocus, EnableWindow, SetDlgItemTextW, SetForegroundWindow, SetActiveWindow, GetDC, FillRect, GetSysColor, GetSysColorBrush, SendMessageW, IsDialogMessageW, GetWindowRect, GetSystemMetrics, SetRect, FindWindowW, IntersectRect, SubtractRect, IsWindow, DestroyWindow, CreateDialogIndirectParamW, CharNextW, MessageBoxW, WaitForInputIdle, GetWindowLongW, SetWindowLongW, GetClientRect, ClientToScreen, SetWindowPos, GetWindowDC, ReleaseDC, EndPaint, BeginPaint, EndDialog, SetWindowTextW, GetDlgItem, ShowWindow, DialogBoxIndirectParamW, GetDesktopWindow, MsgWaitForMultipleObjects, PeekMessageW, wsprintfW, LoadIconW, LoadCursorW, RegisterClassW, CreateWindowExW, GetMessageW, TranslateMessage, DispatchMessageW, DefWindowProcW, PostMessageW, KillTimer, PostQuitMessage, SetTimer, GetDlgCtrlID
GDI32.dll	GetDIBColorTable, GetSystemPaletteEntries, CreatePalette, CreateHalftonePalette, UnrealizeObject, SelectPalette, RealizePalette, CreateFontW, SetBkMode, SetTextColor, GetObjectW, GetDeviceCaps, CreateFontIndirectW, CreateSolidBrush, CreateCompatibleDC, SelectObject, BitBlt, CreateDIBitmap, DeleteDC, DeleteObject, GetStockObject, TranslateCharsetInfo
ADVAPI32.dll	RegEnumKeyW, RegCreateKeyW, LookupPrivilegeValueW, OpenThreadToken, OpenProcessToken, GetTokenInformation, AllocateAndInitializeSid, EqualSid, FreeSid, InitializeSecurityDescriptor, SetSecurityDescriptorOwner, SetSecurityDescriptorGroup, SetSecurityDescriptorDacl, RegEnumKeyExW, RegQueryInfoKeyW, RegDeleteKeyW, RegEnumValueW, RegSetValueExW, RegCreateKeyExW, RegDeleteValueW, RegQueryValueExW, RegOpenKeyExW, RegCloseKey, AdjustTokenPrivileges, RegOpenKeyW
SHELL32.dll	SHGetMalloc, SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, ShellExecuteW, CommandLineToArgvW, SHBrowseForFolderW
ole32.dll	CoTaskMemFree, CoTaskMemRealloc, CoTaskMemAlloc, CLSIDFromProgID, CoInitialize, CoCreateGuid, CreateItemMoniker, GetRunningObjectTable, StringFromGUID2, ProgIDFromCLSID, CoUninitialize, CoInitializeSecurity, CoCreateInstance
OLEAUT32.dll	VariantClear, GetErrorInfo, VarUI4FromStr, SystemTimeToVariantTime, CreateErrorInfo, VarBstrFromDate, SysStringByteLen, LoadTypeLib, RegisterTypeLib, SetErrorInfo, VariantChangeType, SysFreeString, SysAllocStringLen, SysReAllocStringLen, SysStringLen, VarBstrCat, SysAllocString, SysAllocStringByteLen
RPCRT4.dll	UuidToStringW, RpcStringFreeW, UuidFromStringW, UuidCreate

Version Infos

Description	Data
LegalCopyright	Copyright (c) 2013 Flexera Software LLC. All Rights Reserved.
ISInternalVersion	20.0.529
InternalName	Setup

Description	Data
FileVersion	1.20.0001
CompanyName	Star4Live
Internal Build Number	134369
ProductName	Star4Live_P2P
ProductVersion	1.20.0001
FileDescription	Setup Launcher Unicode
ISInternalDescription	Setup Launcher Unicode
OriginalFilename	InstallShield Setup.exe
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:58:24.740777969 CET	53	51281	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:24.805322886 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:24.865369081 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:25.613537073 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:25.665592909 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:26.554683924 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:26.606687069 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:27.579216003 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:27.632970095 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:30.737715960 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:30.788513899 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:33.866300106 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:33.914957047 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:34.990092993 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:35.041727066 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:37.486661911 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:37.538510084 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:38.613193989 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:38.662111044 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:39.826838970 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:39.886837959 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:41.278714895 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:41.332406998 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:42.482049942 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:42.539414883 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:43.708655119 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:43.759005070 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:44.499653101 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:44.551413059 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:45.323533058 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:45.373548031 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:46.416064978 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:46.466809034 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:49.425493002 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:49.478410006 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:58:50.631831884 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:58:50.684979916 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:00.837523937 CET	57084	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:59:00.886444092 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:04.065891981 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:59:04.126425028 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:20.120346069 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:59:20.172939062 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:22.350275993 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:59:22.417875051 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:37.591285944 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:59:37.645448923 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 21:59:40.891699076 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:59:40.949959040 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 22:00:12.078780890 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:00:12.127599955 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 22:00:13.515271902 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:00:13.589353085 CET	53	55435	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Setup.exe PID: 6588 Parent PID: 5704

General

Start time:	21:58:33
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Setup.exe'
Imagebase:	0x400000
File size:	9610518 bytes
MD5 hash:	7B5D30BD9B7CDCCA79E189AAAF5707FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
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	449BCD	CreateDirectoryW
C:\Users\user\AppData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
C:\Users\user\AppData\Local\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
C:\Users\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
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	449BCD	CreateDirectoryW
C:\Users\user\AppData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
C:\Users\user\AppData\Local\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	449BCD	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	449BCD	CreateDirectoryW
C:\Users\user\AppData\Local\Temp_MSI5166._IS	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	44394A	CreateFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	49E74F	CreateFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	6	40A6B3	CreateFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	49E74F	CreateFileW
C:\Users\user\AppData\Local\Temp\~F49E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	444EBD	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\~F4CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	444EBD	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Star4Live_P2P.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	49E74F	CreateFileW
C:\Users\user\Desktop	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4431A6	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4431A6	CreateDirectoryW
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	4431A6	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4431A6	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4431A6	CreateDirectoryW
C:\Users\user\AppData\Local\Downloaded Installations	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4431A6	CreateDirectoryW
C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4431A6	CreateDirectoryW
C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	426E75	CopyFileW
C:\Users\user\AppData\Local\Temp\~FC32.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	444EBD	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp_MSI5166._IS	success or wait	1	443967	DeleteFileW
C:\Users\user\AppData\Local\Temp\~F49E.tmp	success or wait	1	444FC5	DeleteFileW
C:\Users\user\AppData\Local\Temp\~F4CE.tmp	success or wait	1	444FC5	DeleteFileW
C:\Users\user\AppData\Local\Temp\~FC32.tmp	success or wait	1	444FC5	DeleteFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	success or wait	1	443B35	DeleteFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	success or wait	1	443B35	DeleteFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Star4Live_P2P.msi	success or wait	1	443B35	DeleteFileW
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	success or wait	1	443B35	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	unknown	5174	ff fe 5b 00 49 00 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 3d 00 49 00 4e 00 54 00 4c 00 0d 00 0a 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 2e 00 30 00 30 00 2e 00 30 00 30 00 30 00 0d 00 0a 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 3d 00 38 00 30 00 30 00 30 00 09 00 3b 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 20 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 6d 00 65 00 6e 00 74 00 20 00 69 00 6e 00 20 00 4b 00 42 00 0d 00 0a 00 0d 00 0a 00 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 3d 00 0d 00 0a 00 53 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 57 00 72 00 6f 00 6e 00 67 00 4f 00 53 00 3d 00 59 00 0d 00 0a 00 53 00 63 00 72	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=...S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r	success or wait	1	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	2	ff fe	..	success or wait	6	406C0C	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	18	5b 00 46 00 69 00 6c 00 65 00 73 00 5d 00 0d 00 0a 00	[.F.i.l.e.s.].....	success or wait	2	406C0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	unknown	16384	ff fe 5b 00 30 00 78 00 30 00 34 00 30 00 39 00 5d 00 0d 00 0a 00 31 00 31 00 30 00 30 00 3d 00 53 00 65 00 74 00 75 00 70 00 20 00 49 00 6e 00 69 00 74 00 69 00 61 00 6c 00 69 00 7a 00 61 00 74 00 69 00 6f 00 6e 00 20 00 45 00 72 00 72 00 6f 00 72 00 0d 00 0a 00 31 00 31 00 30 00 31 00 3d 00 25 00 73 00 0d 00 0a 00 31 00 31 00 30 00 32 00 3d 00 25 00 31 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 69 00 73 00 20 00 70 00 72 00 65 00 70 00 61 00 72 00 69 00 6e 00 67 00 20 00 74 00 68 00 65 00 20 00 25 00 32 00 2c 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 77 00 69 00 6c 00 6c 00 20 00 67 00 75 00 69 00 64 00 65 00 20 00 79 00 6f 00 75 00 20 00 74 00 68 00 72 00 6f 00 75 00 67 00 68 00 20 00 74 00 68 00 65 00 20 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d	..[.0.x.0.4.0.9.].....1.1.0.0. =.S.e.t.u.p. .I.n.i.t.i.a.l.i. z.a.t.i.o.n. .E.r.r.o.r.....1. 1.0.1.=.%.s.....1.1.0.2.=.%. 1. .S.e.t.u.p. .i.s. .p.r.e.p.a. r.i.n.g. .t.h.e. .%.2.,. .w.h. i.c.h. .w.i.l.l. .g.u.i.d.e. . y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m	success or wait	2	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	18	5b 00 46 00 69 00 6c 00 65 00 73 00 5d 00 0d 00 0a 00	[.F.i.l.e.s.].....	success or wait	3	406C0C	WriteFile
C:\Users\user\AppData\Local\Temp\~F49E.tmp	unknown	5174	ff fe 5b 00 49 00 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 3d 00 49 00 4e 00 54 00 4c 00 0d 00 0a 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 2e 00 30 00 30 00 30 00 30 00 0d 00 0a 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 3d 00 38 00 30 00 30 00 30 00 09 00 3b 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 20 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 6d 00 65 00 6e 00 74 00 20 00 69 00 6e 00 20 00 4b 00 42 00 0d 00 0a 00 0d 00 0a 00 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 3d 00 0d 00 0a 00 53 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 57 00 72 00 6f 00 6e 00 67 00 4f 00 53 00 3d 00 59 00 0d 00 0a 00 53 00 63 00 72	..[.I.n.f.o.].....N.a.m.e.=.I. N.T.L.....V.e.r.s.i.o.n.=.1... 0.0...0.0.0.....D.i.s.k.S.p.a. c.e.=.8.0.0.0...;.D.i.s.k.S.p. a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r. t.u.p.].....C.m.d.L.i.n.e.=... ..S.u.p.p.r.e.s.s.W.r.o.n.g. O.S.=.Y.....S.c.r	success or wait	1	49E909	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~F4CE.tmp	unknown	5174	ff fe 5b 00 49 00 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 3d 00 49 00 4e 00 54 00 4c 00 0d 00 0a 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 2e 00 30 00 30 00 2e 00 30 00 30 00 30 00 0d 00 0a 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 3d 00 38 00 30 00 30 00 30 00 30 00 09 00 3b 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 20 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 6d 00 65 00 6e 00 74 00 20 00 69 00 6e 00 20 00 4b 00 42 00 0d 00 0a 00 0d 00 0a 00 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 3d 00 0d 00 0a 00 53 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 57 00 72 00 6f 00 6e 00 67 00 4f 00 53 00 3d 00 59 00 0d 00 0a 00 53 00 63 00 72	..[.I.n.f.o.].....N.a.m.e.=.I.N.T.L.....V.e.r.s.i.o.n.=.1...0.0...0.0.0.....D.i.s.k.S.p.a.c.e.=.8.0.0.0.0...;.D.i.s.k.S.p.a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.....[.S.t.a.r.t.u.p.].....C.m.d.L.i.n.e.=...S.u.p.p.r.e.s.s.W.r.o.n.g.O.S.=.Y.....S.c.r	success or wait	1	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Star4Live_P2P.msi	unknown	16384	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 00 00 00 00 00 00 10 00 00 38 00 00 00 05 00 00 00 80 36 00 00 01 00 00 00 00 00 00 00 80 00 00 00 da 00 00 00 80 01 00 00 ff 01 00 00 7f 02 00 00 00 03 00 00 7f 03 00 00 00 04 00 00 80 04 00 00 ff 04 00 00 80 05 00 00 00 06 00 00 7f 06 00 00 00 07 00 00 7f 07 00 00 00 08 00 00 7f 08 00 00 00 09 00 00 7f 09 00 00 00 0a 00 00 7f 0a 00 00 00 0b 00 00 7f 0b 00 00 00 0c 00 00 7f 0c 00 00 00 0d 00 00 7f 0d 00 00 00 0e 00 00 7f 0e 00 00 00 0f 00 00 7f 0f 00 00 00 10 00 00 7f 10 00 00 00 11 00 00 7f 11 00 00 00 12 00 00 7f 12 00 00 00 13 00 00 7f 13 00 00 00 14 00 00 7f 14 00 00 00 15 00 00 7f 15 00 00 00 16 00	.....>..... ..... 8.....6.....	success or wait	748	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Star4Live_P2P.msi	unknown	0			success or wait	3	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	18	5b 00 46 00 69 00 6c 00 65 00 73 00 5d 00 0d 00 0a 00	[.F.i.l.e.s.].....	success or wait	4	406C0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi	0	1048576	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 38 00 00 00 05 00 00 00 80 36 00 00 01 00 00 00 00 00 00 00 80 00 00 00 da 00 00 00 80 01 00 00 ff 01 00 00 7f 02 00 00 00 03 00 00 7f 03 00 00 00 04 00 00 80 04 00 00 ff 04 00 00 80 05 00 00 00 06 00 00 7f 06 00 00 00 07 00 00 7f 07 00 00 00 08 00 00 7f 08 00 00 00 09 00 00 7f 09 00 00 00 0a 00 00 7f 0a 00 00 00 0b 00 00 7f 0b 00 00 00 0c 00 00 7f 0c 00 00 00 0d 00 00 7f 0d 00 00 00 0e 00 00 7f 0e 00 00 00 0f 00 00 7f 0f 00 00 00 10 00 00 7f 10 00 00 00 11 00 00 7f 11 00 00 00 12 00 00 7f 12 00 00 00 13 00 00 7f 13 00 00 00 14 00 00 7f 14 00 00 00 15 00 00 7f 15 00 00 00 16 00	........................>..... .... 8........6....................	success or wait	9	426E75	CopyFileW
C:\Users\user\AppData\Local\Temp\~FC32.tmp	unknown	5174	ff fe 5b 00 49 00 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4e 00 61 00 6d 00 65 00 3d 00 49 00 4e 00 54 00 4c 00 0d 00 0a 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 2e 00 30 00 30 00 2e 00 30 00 30 00 30 00 0d 00 0a 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 3d 00 38 00 30 00 30 00 30 00 09 00 3b 00 44 00 69 00 73 00 6b 00 53 00 70 00 61 00 63 00 65 00 20 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 6d 00 65 00 6e 00 74 00 20 00 69 00 6e 00 20 00 4b 00 42 00 0d 00 0a 00 0d 00 0a 00 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 3d 00 0d 00 0a 00 53 00 75 00 70 00 70 00 72 00 65 00 73 00 73 00 57 00 72 00 6f 00 6e 00 67 00 4f 00 53 00 3d 00 59 00 0d 00 0a 00 53 00 63 00 72	..[.I.n.f.o.].....N.a.m.e.=.I. N.T.L.....V.e.r.s.i.o.n.=.1... 0.0...0.0.0.....D.i.s.k.S.p.a. c.e.=.8.0.0.0...;.D.i.s.k.S.p. a.c.e. .r.e.q.u.i.r.e.m.e.n.t. .i.n. .K.B.........[.S.t.a.r. t.u.p.].....C.m.d.L.i.n.e.=... ..S.u.p.p.r.e.s.s.W.r.o.n.g. O.S.=.Y.....S.c.r	success or wait	1	49E909	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	18	5b 00 46 00 69 00 6c 00 65 00 73 00 5d 00 0d 00 0a 00	[.F.i.l.e.s.].....	success or wait	4	406C0C	WriteFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	18	5b 00 46 00 69 00 6c 00 65 00 73 00 5d 00 0d 00 0a 00	[.F.i.l.e.s.].....	success or wait	2	406C0C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Setup.exe	unknown	46	success or wait	1	4429B5	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	24	success or wait	2	4422FF	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	16384	success or wait	1	440FBA	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	unknown	2	success or wait	1	437F7D	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	unknown	5174	success or wait	1	44CE73	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	16384	success or wait	1	440FBA	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	1024	success or wait	9	4060A5	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}_ISMSIDEL.INI	unknown	208	success or wait	9	409C34	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\Setup.INI	unknown	1024	success or wait	1	4060A5	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	unknown	2	success or wait	14	437F7D	ReadFile
C:\Users\user\AppData\Local\Temp\{429B5CB3-339E-483B-9032-CB0DA14F2F9A}\0x0409.ini	unknown	22492	success or wait	14	44CE73	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	46	success or wait	3	4429B5	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	16384	success or wait	3	440FBA	ReadFile
C:\Users\user\AppData\Local\Temp\~F49E.tmp	unknown	1024	success or wait	1	4060A5	ReadFile
C:\Users\user\AppData\Local\Temp\~F49E.tmp	unknown	5174	success or wait	1	409C34	ReadFile
C:\Users\user\AppData\Local\Temp\~F4CE.tmp	unknown	1024	success or wait	1	4060A5	ReadFile
C:\Users\user\AppData\Local\Temp\~F4CE.tmp	unknown	5174	success or wait	1	409C34	ReadFile
C:\Users\user\Desktop\Setup.exe	unknown	16384	success or wait	512	440FBA	ReadFile
C:\Users\user\AppData\Local\Temp\~FC32.tmp	unknown	1024	success or wait	1	4060A5	ReadFile
C:\Users\user\AppData\Local\Temp\~FC32.tmp	unknown	5174	success or wait	1	409C34	ReadFile

Analysis Process: svchost.exe PID: 6600 Parent PID: 568

General

Start time:	21:58:32
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: msiexec.exe PID: 6708 Parent PID: 6588

General

Start time:	21:58:39
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	MSIEXEC.EXE /i 'C:\Users\user\AppData\Local\Downloaded Installations\{877F9BE8-C6E2-462D-9A96-09E42390D002}\Star4Live_P2P.msi' SETUPEXEDIR='C:\Users\user\Desktop' SETUPEXENAME='Setup.exe'
Imagebase:	0xd10000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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 Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6764 Parent PID: 2224

General

Start time:	21:58:41
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding C31728C15F7B7E0360F95AF524D72042 C
Imagebase:	0xd10000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: 7052 Parent PID: 2224

General

Start time:	21:58:50
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 9ADD54B1DEB9106D315583847C272BCA
Imagebase:	0xd10000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: CloudHttpWin32Server.exe PID: 7100 Parent PID: 568

General

Start time:	21:58:51
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWin32Server.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWin32Server.exe

Imagebase:	0xcf0000
File size:	11264 bytes
MD5 hash:	5921172EC58195BD404999F1D46A6867
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7120 Parent PID: 7100

General

Start time:	21:58:51
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpServer.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 7148 Parent PID: 7120

General

Start time:	21:58:51
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: taskkill.exe PID: 6100 Parent PID: 7120

General

Start time:	21:58:52
Start date:	25/02/2021

Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /F /IM CloudHttpServer.exe
Imagebase:	0xdc0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5364 Parent PID: 7100

General

Start time:	21:58:52
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpWindowPopup.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 4084 Parent PID: 5364

General

Start time:	21:58:52
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: taskkill.exe PID: 1004 Parent PID: 5364

General

Start time:	21:58:53
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /F /IM CloudHttpWindowPopup.exe
Imagebase:	0xdc0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: CloudHttpServer.exe PID: 1636 Parent PID: 7100

General

Start time:	21:58:53
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpServer.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpServer.exe
Imagebase:	0x240000
File size:	35840 bytes
MD5 hash:	FC73EBB8FB9E3B9520CE0516E778B6B9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: CloudHttpWindowPopup.exe PID: 6052 Parent PID: 7100

General

Start time:	21:58:53
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWindowPopup.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Star4Live\Star4Live_P2P\CloudHttpWindowPopup.exe
Imagebase:	0x3d0000
File size:	67584 bytes
MD5 hash:	C67AA650D57D92A0CF805343593C6AB9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6312 Parent PID: 1636

General

Start time:	21:58:53
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: conhost.exe PID: 6224 Parent PID: 6052

General

Start time:	21:58:54
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: cmd.exe PID: 3980 Parent PID: 7100

General

Start time:	21:58:54
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpServer.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 2992 Parent PID: 3980

General

Start time:	21:58:54
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: taskkill.exe PID: 6184 Parent PID: 3980

General

Start time:	21:58:54
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /F /IM CloudHttpServer.exe
Imagebase:	0xdc0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6152 Parent PID: 7100

General

Start time:	21:58:55
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c taskkill /F /IM CloudHttpWindowPopup.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6208 Parent PID: 6152

General

Start time:	21:58:55
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: taskkill.exe PID: 6404 Parent PID: 6152

General

Start time:	21:58:56
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /F /IM CloudHttpWindowPopup.exe
Imagebase:	0xdc0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6340 Parent PID: 568

General

Start time:	21:59:01
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6724 Parent PID: 568

General

Start time:	21:59:01
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7012 Parent PID: 568

General

Start time:	21:59:12
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7032 Parent PID: 568

General

Start time:	21:59:13
Start date:	25/02/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5324 Parent PID: 568

General

Start time:	21:59:13
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4472 Parent PID: 568

General

Start time:	21:59:13
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6104 Parent PID: 568

General

Start time:	21:59:14
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 1744 Parent PID: 568

General

Start time:	21:59:14
Start date:	25/02/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff779450000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5368 Parent PID: 568

General

Start time:	21:59:15
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6172 Parent PID: 568

General

Start time:	21:59:15
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis