ID: 679294
Sample Name: ORDINE.exe
Cookbook: default.jbs
Time: 14:46:13
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report ORDINE.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: AsyncRAT 4
Yara Signatures 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 6
Boot Survival 6
Malware Analysis System Evasion 7
Anti Debugging 7
HIPS / PFW / Operating System Protection Evasion 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 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDINE.exe.log 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iexplore.exe.log 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log 12
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe 13
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe:Zone.Identifier 13
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 16
Sections 16
Resources 16
Imports 17
Possible Origin 17
Network Behavior 17
Snort IDS Alerts 17
TCP Packets 17
Statistics 19
Behavior 19

System Behavior 19
Analysis Process: ORDINE.exePID: 5760, Parent PID: 5552 19
General 19
File Activities 20
Analysis Process: vbc.exePID: 1164, Parent PID: 5760 20
General 20
File Activities 20
File Created 20
File Read 20
Analysis Process: cmd.exePID: 3472, Parent PID: 5760 21
General 21
File Activities 21
File Created 21
Analysis Process: conhost.exePID: 5496, Parent PID: 3472 21
General 21
Analysis Process: cmd.exePID: 5416, Parent PID: 5760 22
General 22
File Activities 22
Analysis Process: conhost.exePID: 5748, Parent PID: 5416 22
General 22
Analysis Process: cmd.exePID: 5736, Parent PID: 5760 22
General 22
File Activities 23
File Created 23
File Written 23
File Read 23
Analysis Process: schtasks.exePID: 6000, Parent PID: 5416 23
General 23
File Activities 24
Analysis Process: conhost.exePID: 5408, Parent PID: 5736 24
General 24
Analysis Process: iexplore.exePID: 2848, Parent PID: 1040 24
General 24
File Activities 24
File Created 24
File Written 25
File Read 25
Analysis Process: vbc.exePID: 5660, Parent PID: 2848 25
General 25
File Activities 26
File Created 26
File Written 26
File Read 26
Analysis Process: cmd.exePID: 4976, Parent PID: 2848 27
General 27
File Activities 27
File Created 27
Analysis Process: conhost.exePID: 5400, Parent PID: 4976 27
General 27
Analysis Process: cmd.exePID: 2432, Parent PID: 2848 27
General 27
File Activities 28
Analysis Process: conhost.exePID: 3408, Parent PID: 2432 28
General 28
Analysis Process: cmd.exePID: 4448, Parent PID: 2848 28
General 28
File Activities 28
File Read 28
Analysis Process: schtasks.exePID: 5348, Parent PID: 2432 29
General 29
File Activities 29
Analysis Process: conhost.exePID: 4512, Parent PID: 4448 29
General 29
Analysis Process: BackgroundTransferHost.exePID: 2432, Parent PID: 812 29
General 29
File Activities 29
Analysis Process: iexplore.exePID: 4604, Parent PID: 1040 30
General 30
File Activities 30
File Created 30
File Read 30
Disassembly 30

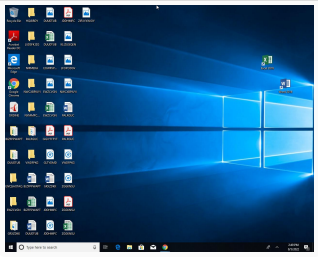
Windows Analysis Report

ORDINE.exe

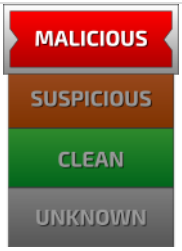
Overview

General Information

Sample Name:	ORDINE.exe
Analysis ID:	679294
MD5:	30e619eed663b6.
SHA1:	04ad1454bb163c..
SHA256:	faaddcf1294c835..
Tags:	AsyncRAT exe RAT
Infos:	



Detection



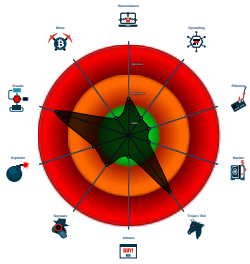
AsyncRAT

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

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Injects files into Windows application
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Binary or sample is protected by do…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- ORDINE.exe (PID: 5760 cmdline: "C:\Users\user\Desktop\ORDINE.exe" MD5: 30E619EED663B6696BA1269DEC11E1A9)
  - vbc.exe (PID: 1164 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - cmd.exe (PID: 3472 cmdline: cmd" /c mkdir "C:\Users\user\AppData\Local\Temp\iexplore MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5416 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6000 cmdline: schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 5736 cmdline: cmd" /c copy "C:\Users\user\Desktop\ORDINE.exe" "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- iexplore.exe (PID: 2848 cmdline: C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe MD5: 30E619EED663B6696BA1269DEC11E1A9)
  - vbc.exe (PID: 5660 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - cmd.exe (PID: 4976 cmdline: cmd" /c mkdir "C:\Users\user\AppData\Local\Temp\iexplore MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2432 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5348 cmdline: schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 4448 cmdline: cmd" /c copy "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - BackgroundTransferHost.exe (PID: 2432 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
- iexplore.exe (PID: 4604 cmdline: C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe MD5: 30E619EED663B6696BA1269DEC11E1A9)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "191.101.130.243",
  "Ports": "7707",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "AES_key": "F37wL6kU6d1ln0ZzFzD1Z61sP0kXqYbm",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "Certificate":
"MIIE8jCCAtqgAwIBAgIQALjgwS++igAkwAOyv5bgMTANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjIwODAzMDYwMjIyWhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAILRFbpKGfwFx25WYYuVCgXl7TdoxRlXM7zcKGvdFLIDy1Bwzp0Y99L/Yy/oseRDrfihrsyph3Ms454cgfjFob5XtBvoXtPAO32uamRVh+1y+C67eBmRe/MTSmTHmQsttSmFFVBwfl5rSS3q2lhTvhPSyQlNn2Y9TAvIIqrg0gIYOW65cTGikiV1+8P+sOoCH9JWRcNUKSrTDX0O+6ZCTOc3UKBW5oj//FcsGreSZw7E2mMTX5WHJNIB5zXB6cfpPdQBwpvJWnpWfCaMgEuJdRC6EznuC0ZFfxQSSCiH8ZkS+JC/MtA/WGWHggqPo/dywuLNygPleYVxK0tVPSZTFEH7Mpo7Z+TiVL6xno7y3LtuaAUvP+yddJ/rhQOmHbs6Qn9zpV39WXz4K3JBp+OYhHUCWpPfjnE9eR4xLzwK2RfwPGhbboIj7TgAdl3YHa9R+sSM19PXHNQjXRMxoZ32Em8EmdSqzbN0lW+I+7/hc+42J22p+fKOnuC2CiBUBNk5ODph27qZ65UYRywRJIkZnCz6K9VDSeDTmF8BrlxdC89mtidHBe9s+ZmBrK4hsJ7VigYXN1J5s9aiaEmfLIGfG1mzv2f9/9Dly4k0tAx9K0PgZmpHBw6HWFjj/88CKy954G2Lb9KJNRyOLLPNs9e4eh8jWEinryjA+0RG0bxlqfdJAgMBAAGjMjAwMB0GA1UdDgQWBBSTNFdMcn6A/QRYYvQpa7SIp9dQQDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4ICAQAEhlXRdBaUw7zIzKsy1KHQ5goP0TMTkmw+cP2ufXJGYE1rMRHCz9CTAPCd+OSjjzljF8sVUY403LxZdaAI0wB+6RG/3gLcMhljO83Xegx0uONr50r1VAWYwbQU/qQdzsX2epdgqt3S6d0DFzfXE68V0lXL7Plw/Bc3qlrborgVfSHpdWCTCgcJ4a8YDsA+6wi3uADUlm52ztAveJ9f7IYUk7XzevOKqsqmHt+xmWFqgiw1DWvdAx+qDYfXnko8ypz10uffTNahU82eUiD96TBJt0Gr+d5tfPLmt1yTYa0XzxWy0r9dvYZWEbV5r03Ce2cw26V3z77OX6ZvckR1/qG0tIL06V8nXhmhV0zGGK1i9by9vivfBFQxD2EcVUyPL4URLpDoCqipskOo4bt2TLqUzssOkH41l8n6yZJl8/xYFyzH/2hfY1VS6NnLd9J2w0+ToHxXlhpwZb58JOVXSavCF6d/767aBg8v+Y+MH17RTjBuB+gk7qoJLKGqyTAhag3GvQ9aMVLBxNT99JBcmyUO/3NMTDt4ckAUpEuImvo1zvPdRZV+VnmQbfTBynoWXfw1cDPc+qfE2gS55hMhk/vitY9h4fy/AbcXtwb4+Diok6tOMQ32aHVws9ForCAGEKldMlus0/+WTTpqwwgmO38oegFS6GzWA3PpYUedJXTE2g==",
  "ServerSignature":
"LnD03k7cpYYvIPzVlgkFIKRQeIVSCNDslUHUMdlARBBMyw1TZMPHK9AU16GUATrv8GN6kBdJLY0QW7A/k2nEAOJPZxlNYr02XeXsdcOs4sqLfeKPYe2250zmeejLRoK8Ycov9Eks1PKGHs4jCsX/nVTmoUjPMCjEav/y5ZWKHhMYlq0kYRdgpJdRJ1kFNqoq+OhbbizKo/z+3HCVLhI3vtIqg7opzzqCrVELXFDiwRMHKt5QNjXoyKd7jvjcmDIHbNfO05ZTmF8P624rLX1x7/Z4eZEorwOSwHqTbY9t05liSFDY0xzY8Iwjx2ci6+kKP/u3Gu9jqX4lPEulNxweH+pNLpuSzxcKhLr13jkK4Gh/jz3B4L3XB2qOzo8p6Ct/Yos3DaKUHvswTfBRY7yCyHxnvWL8bxgInaQ5nXzhqTz0EcbngcX6tJYI+pRb+db/HJeF2HsiqwFHv+074+iDOan6/yyoyjaQybCmfggxaFtknvnJW8oU+aiBZAsH8ONvOVhG3wKs/fwBrND+5MPyALU61tvQK9/KY1/JCSmTD/wtUiAyXUmp3nfZ+Wc5ZSH+D39TOMVFv0u47JE0gDFoP23TyGvBBGPc2cyH86dCznzrIfqsIxOh6IQ6Fj4u9E7Mf7CHVIBjSGw//UzjI5r9DhyATGXHGkyFoHquvUk+soc=",
  "BDOS": "false",
  "Startup_Delay": "3",
  "Group": "Alibaba"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x102bf2:$x1: AsyncRAT • 0x102c30:$x1: AsyncRAT

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.534970060.0000000008E76000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x8243:$x1: AsyncRAT • 0x8281:$x1: AsyncRAT
00000026.00000002.692124542.00000000035F2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000026.00000002.692124542.00000000035F2000.00000004.00000800.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0xa65d:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
00000006.00000002.681364140.00000000051A3000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x35f93:$x1: AsyncRAT • 0x35fd1:$x1: AsyncRAT • 0x56ef7:$x1: AsyncRAT • 0x56f35:$x1: AsyncRAT
0000000E.00000002.522558294.0000000002AD4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Click to see the 17 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.vbc.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
6.0.vbc.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
6.0.vbc.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x99c1:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Generic AsyncRAT Style SSL Cert - Source IP: 191.101.130.243 - Destination IP: 192.168.2.5

Timestamp:	191.101.130.243192.168.2.57707497642035595 08/05/22-14:47:38.477674
SID:	2035595
Source Port:	7707
Destination Port:	49764
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server) - Source IP: 191.101.130.243 - Destination IP: 192.168.2.5

Timestamp:	191.101.130.243192.168.2.57707497642030673 08/05/22-14:47:38.477674
SID:	2030673
Source Port:	7707
Destination Port:	49764
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Binary or sample is protected by dotNetProtector

.NET source code contains potential unpacker

Boot Survival

Yara detected AsyncRAT

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

Malware Analysis System Evasion

Yara detected AsyncRAT

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

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

Injects files into Windows application

Writes to foreign memory regions

Injects a PE file into a foreign processes

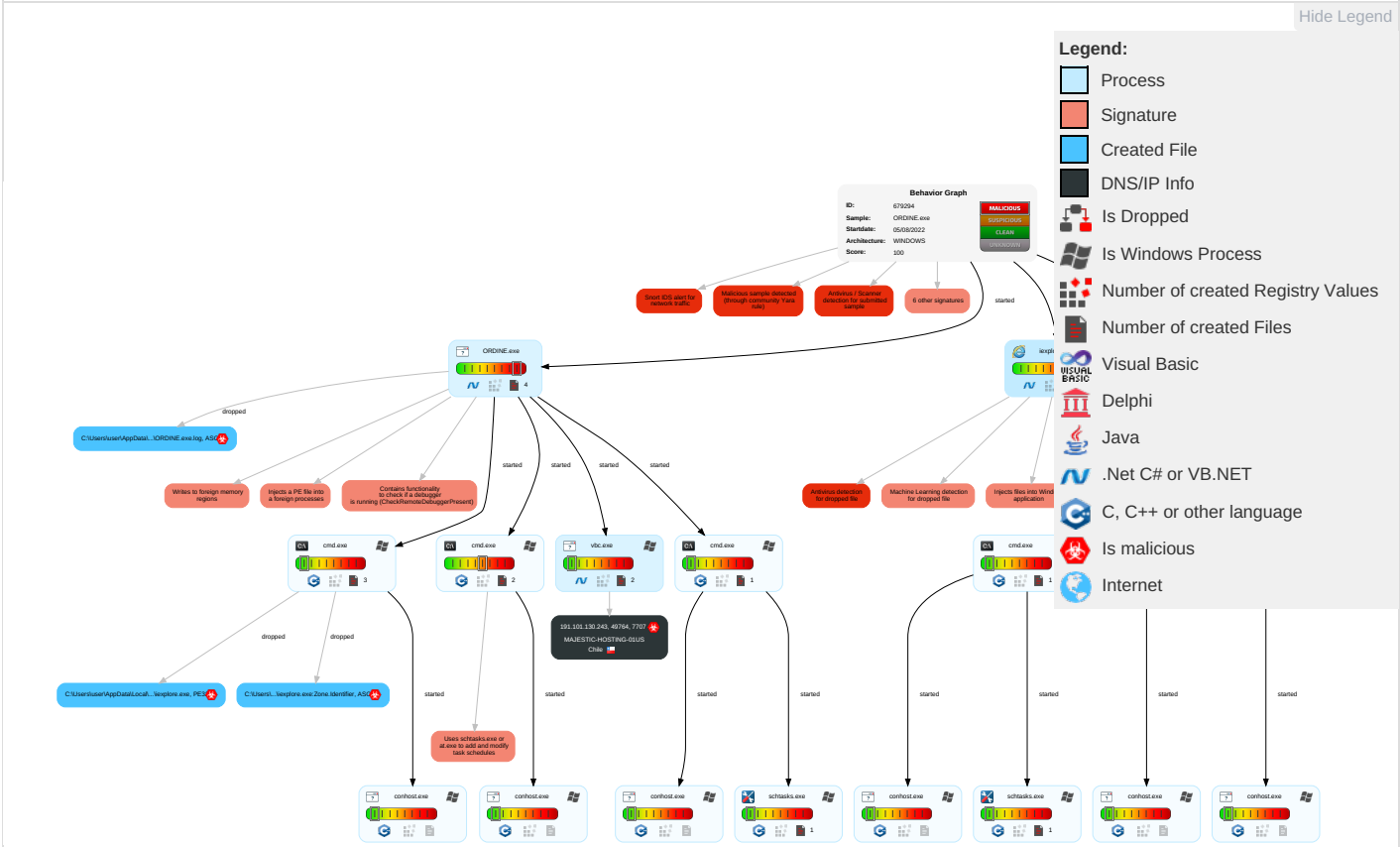
Lowering of HIPS / PFW / Operating System Security Settings

Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Scheduled Task/Job	2 Scheduled Task/Job	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	3 1 2 Process Injection	1 Access Token Manipulation	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Exploitation for Client Execution	Logon Script (Mac)	2 Scheduled Task/Job	1 Disable or Modify Tools	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 2 Process Injection	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

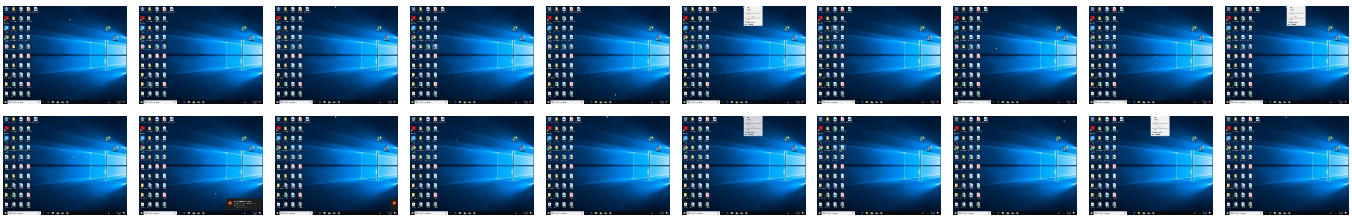
Behavior Graph



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
ORDINE.exe	100%	Avira	TR/Dropper.Gen	
ORDINE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202836		Download File
14.0.iexplore.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1230579		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

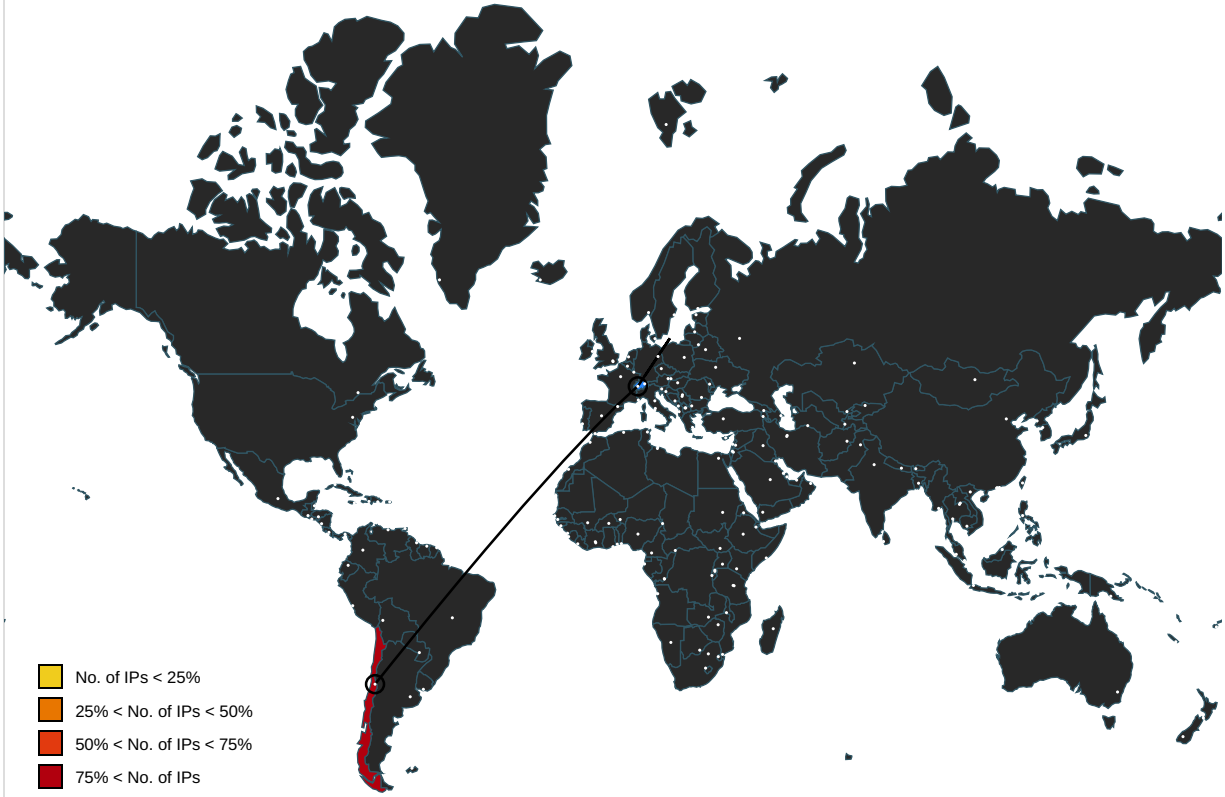
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000006.00000002.683833759.0000006BD4000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.101.130.243	unknown	Chile		396073	MAJESTIC-HOSTING-01US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679294
Start date and time: 05/08/202214:46:13	2022-08-05 14:46:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 32s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	ORDINE.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:	MAL
Classification:	mal100.troj.evad.winEXE@30/5@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:47:36	Task Scheduler	Run new task: Nafifas path: "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDINE.exe.log

Process:	C:\Users\user\Desktop\ORDINE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iexplore.exe.log

Process:	C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101

SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3145728
Entropy (8bit):	1.1807463156564255
Encrypted:	false
SSDEEP:	6144:PnsnxlpI/4MgsaffkOiBxqwuhiowOskDnlat1JLfwyTeiB0PJo3zzn:fs3pZ4MgzffDwsbikcJpnfn
MD5:	30E619EED663B6696BA1269DEC11E1A9
SHA1:	04AD1454BB163C8E1C5820BA591AE613DD6F6D45
SHA-256:	FAADDCF1294C8358FC6CCC4C36ECDC9FCCD03AC345B3D022DB144798D611397D
SHA-512:	2C7FF7B8658137E4C1CE494B2944E41C51BE8C5D163DF07CC3B16736D3ABF591EA530D2B4B5FCA212FC96D72383A4E65BFE42491A938DC12B42E78B764439B3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... ..b.....~.... .....@.. ....@.....0...K.....r..... ....H.....text..... ....`.rsrc...r.....@..@.reloc..... .....L.....@..B.....`.....H.....<.....3....4.....Ivan Meedev...(....*..-.*(....&*2~.....(....*..(....*.*..{....*..{....*:~.....(....*..{....*..{....*:~.....(....*6~.....(....*..{....*..{....*..{....*..{....*..{....*.~....(....*.~S...(....*..{....*..{....*.~....(....*..{....*..{....*..{....*.~8...(....*..{....*6~H.....(....*6~I.....(....*..0..?.....#E...v.c@#..... S@(o...Y(p...(.....#.....t@#.....[@(q...Y(p...($.....#....

C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	1.1807463156564255
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ORDINE.exe
File size:	3145728
MD5:	30e619eed663b6696ba1269dec11e1a9
SHA1:	04ad1454bb163c8e1c5820ba591ae613dd6f6d45
SHA256:	faaddcf1294c8358fc6ccc4c36ecdc9fccd03ac345b3d022db144798d611397d
SHA512:	2c7ff7b8658137e4c1ce494b2944e41c51be8c5d163df07cc3b16736d3abf591ea530d2b4b5fca212fc96d72383a4e65bfe42491a938dc12b42e78b764439bb3

SSDEEP:	6144:Pnsnxlpl/4MgsaffkOiBxqwuhiowOskDnlat1JLfwyTeiB0PJo3zzn:fs3pZ4MgzffDwsbikcJpnfn
TLSH:	C3E5DE3C37F13B61EC9DC831468165246BEA0FA7DEA186D1D3EA19C7930D8F52D44A8B
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L... ..b............................~.... ....@.. ....@................................

File Icon

	
Icon Hash:	74f4d8cccaccdce4

Static PE Info

General

Entrypoint:	0x44a87e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62ECB720 [Fri Aug 5 06:22:24 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4a830	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c000	0x2bf72	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x78000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x48884	0x48a00	False	0.42609052280550774	data	5.630156495500773	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x2bf72	0x2c000	False	0.217041015625	data	4.522066472641785	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c2c4	0x3b4b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x4fe10	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x60638	0x94a8	data		
RT_ICON	0x69ae0	0x5488	data		
RT_ICON	0x6ef68	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 49407, next used block 4294902528		
RT_ICON	0x73190	0x25a8	data		
RT_ICON	0x75738	0x10a8	data		
RT_ICON	0x767e0	0x988	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x77168	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x775d0	0x84	data		
RT_VERSION	0x77654	0x1f8	data	English	United States
RT_MANIFEST	0x7784c	0x726	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
191.101.130.243192.168.2.57707497642035595 08/05/22-14:47:38.477674	TCP	2035595	ET TROJAN Generic AsyncRAT Style SSL Cert	7707	49764	191.101.130.243	192.168.2.5
191.101.130.243192.168.2.57707497642030673 08/05/22-14:47:38.477674	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	7707	49764	191.101.130.243	192.168.2.5

TCP Packets

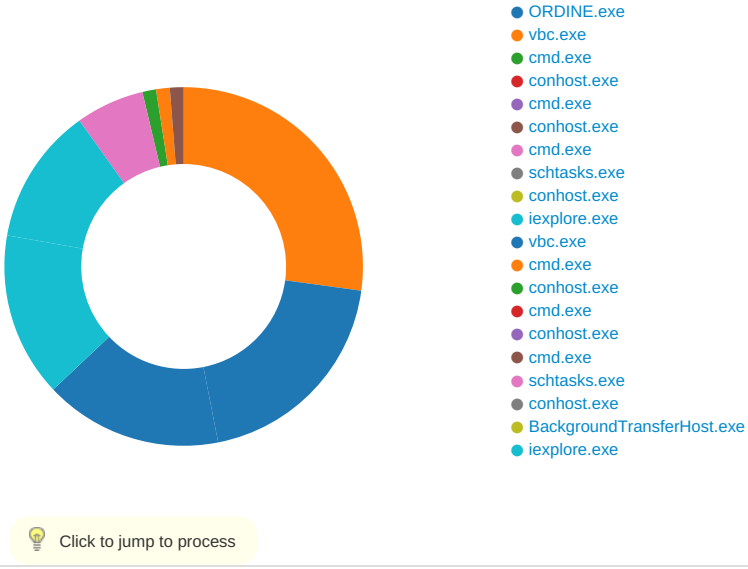
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:47:38.127145052 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:38.269309998 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:38.269445896 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:38.318298101 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:38.477674007 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:38.477732897 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:38.477982998 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:38.487781048 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:38.640578032 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:38.751085043 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:40.419425011 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:40.615670919 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:40.618067026 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:40.809494972 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:50.430208921 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:50.623672009 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:50.623825073 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:50.766381025 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:50.970876932 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:51.112742901 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:51.252288103 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:51.692173004 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:47:51.884382963 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:47:51.884573936 CEST	49764	7707	192.168.2.5	191.101.130.243

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:47:52.077028036 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:00.474582911 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:00.666841030 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:00.667256117 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:00.810467958 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:00.956156969 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:01.098112106 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:01.102432966 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:01.294476986 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:01.295002937 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:01.487618923 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:06.666898012 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:06.753413916 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:06.895541906 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:06.956677914 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:10.521596909 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:10.714154959 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:10.714251041 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:10.857007980 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:10.960084915 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:11.105015039 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:11.109167099 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:11.300544977 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:11.300617933 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:11.492717028 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:20.573885918 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:20.766634941 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:20.766736031 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:20.909015894 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:20.957745075 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:21.099809885 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:21.107994080 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:21.299247980 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:21.299333096 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:21.491667986 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:30.627182961 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:30.819617033 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:30.824776888 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:31.017733097 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:31.100992918 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:31.144403934 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:31.286057949 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:31.294070005 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:31.486768007 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:31.489630938 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:31.681834936 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:36.670231104 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:36.858855009 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:36.996824026 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:37.014642954 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:37.014746904 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:40.674314976 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:40.865524054 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:40.865680933 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:41.007802010 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:41.156017065 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:41.297467947 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:41.303443909 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:41.495160103 CEST	7707	49764	191.101.130.243	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 14:48:41.495237112 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:41.687614918 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:50.721977949 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:50.913625956 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:50.913796902 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:51.106523037 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:51.119471073 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:51.360080004 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:51.501856089 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:51.512048006 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:51.704071045 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:48:51.705694914 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:48:51.899034023 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:49:00.770054102 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:49:00.962053061 CEST	7707	49764	191.101.130.243	192.168.2.5
Aug 5, 2022 14:49:00.964544058 CEST	49764	7707	192.168.2.5	191.101.130.243
Aug 5, 2022 14:49:01.107496977 CEST	7707	49764	191.101.130.243	192.168.2.5

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ORDINE.exe PID: **5760**, Parent PID: **5552**

General

Target ID:	0
Start time:	14:47:18
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\ORDINE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ORDINE.exe"
Imagebase:	0x960000
File size:	3145728 bytes
MD5 hash:	30E619EED663B6696BA1269DEC11E1A9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.454482675.0000000002A86000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.454482675.0000000002A86000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

Analysis Process: vbc.exe PID: 1164, Parent PID: 5760

General

Target ID:	6
Start time:	14:47:30
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xd90000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000006.00000002.681364140.00000000051A3000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.438076644.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000000.438076644.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.683833759.0000000006BD4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000006.00000002.683833759.0000000006BD4000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D875705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D87CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D87CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D87CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D875705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	success or wait	1	6C6E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	end of file	1	6C6E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D875705	unknown

Analysis Process: cmd.exe PID: **3472**, Parent PID: **5760**

General

Target ID:	7
Start time:	14:47:32
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c mkdir "C:\Users\user\AppData\Local\Temp\iexplore
Imagebase:	0x1100000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iexplore	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	110BFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **5496**, Parent PID: **3472**

General

Target ID:	8
Start time:	14:47:33
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **5416**, Parent PID: **5760**

General

Target ID:	9
Start time:	14:47:33
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Imagebase:	0x1100000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5748**, Parent PID: **5416**

General

Target ID:	10
Start time:	14:47:34
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **5736**, Parent PID: **5760**

General

Target ID:	11
Start time:	14:47:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\Desktop\ORDINE.exe" "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Imagebase:	0x1100000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe	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	1104E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	1104E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 20 fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 04 00 00 fd 02 00 00 00 00 00 7e fd 04 00 00 20 00 00 00 fd 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 07 00 00 02 00 00 fd fd 07 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL b~ @ @	success or wait	6	1104E97	CopyFileExW
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	1104E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ORDINE.exe	unknown	512	success or wait	1	1105742	ReadFile

Analysis Process: schtasks.exe PID: **6000**, Parent PID: **5416**

General

Target ID:	12
Start time:	14:47:34
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Imagebase:	0x320000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5408**, Parent PID: **5736**

General

Target ID:	13
Start time:	14:47:35
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: iexplore.exe PID: **2848**, Parent PID: **1040**

General

Target ID:	14
Start time:	14:47:36
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Imagebase:	0x3c0000
File size:	3145728 bytes
MD5 hash:	30E619EED663B6696BA1269DEC11E1A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000002.522558294.0000000002AD4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iexplore.exe.log	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6DBAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iexplore.exe.log	0	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DBAC907	WriteFile

File Read

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

Analysis Process: vbc.exe PID: **5660**, Parent PID: **2848**

General

Target ID:	20
Start time:	14:48:00
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xd90000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000014.00000002.534970060.0000000008E76000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000014.00000002.527812189.00000000069C1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log	0	425	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DBAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D875705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D87CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D87CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D87CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D875705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D875705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7D03DE	ReadFile

Analysis Process: cmd.exe PID: **4976**, Parent PID: **2848**

General

Target ID:	21
Start time:	14:48:02
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c mkdir "C:\Users\user\AppData\Local\Temp\iexplore
Imagebase:	0x1100000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iexplore	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	110BFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **5400**, Parent PID: **4976**

General

Target ID:	22
Start time:	14:48:03
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2432**, Parent PID: **2848**

General

Target ID:	23
Start time:	14:48:03
Start date:	05/08/2022

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3408**, Parent PID: **2432**

General

Target ID:	24
Start time:	14:48:04
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4448**, Parent PID: **2848**

General

Target ID:	25
Start time:	14:48:04
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe" "C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Imagebase:	0x1100000
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe	unknown	512	success or wait	1	1105742	ReadFile

Analysis Process: schtasks.exe PID: **5348**, Parent PID: **2432**

General	
Target ID:	26
Start time:	14:48:05
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe'" /f
Imagebase:	0x320000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4512**, Parent PID: **4448**

General	
Target ID:	27
Start time:	14:48:05
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: BackgroundTransferHost.exe PID: **2432**, Parent PID: **812**

General	
Target ID:	34
Start time:	14:48:34
Start date:	05/08/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff6e0560000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: **4604**, Parent PID: **1040**

General

Target ID:	38
Start time:	14:49:01
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\iexplore\iexplore.exe
Imagebase:	0x3c0000
File size:	3145728 bytes
MD5 hash:	30E619EED663B6696BA1269DEC11E1A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000026.00000002.692124542.00000000035F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000026.00000002.692124542.00000000035F2000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D89CF06	unknown

File Read

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

Disassembly

No disassembly