ID: 745562
Sample Name: ts.exe_
Cookbook: default.jbs
Time: 14:05:50
Date: 14/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

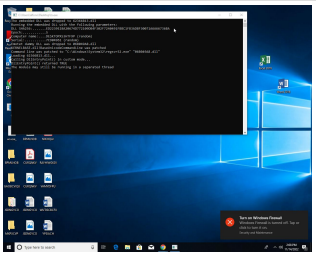
Windows Analysis Report

ts.exe_

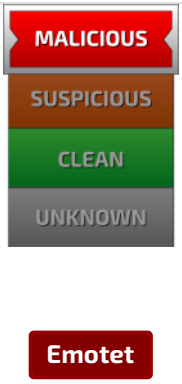
Overview

General Information

Sample Name:	ts.exe_ (renamed file extension from exe_ to exe)
Analysis ID:	745562
MD5:	ad57d446c107b5..
SHA1:	8e277fb9bc97be..
SHA256:	58d9d7c2d4a414..
Infos:	



Detection



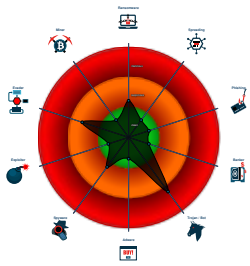
Emotet

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Malicious sample detected (through…
- Antivirus detection for dropped file
- Machine Learning detection for sam…
- PE file does not import any functions
- Yara signature match
- Drops PE files
- Contains functionality to check if a d…
- Contains functionality to query local…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- ts.exe (PID: 3664 cmdline: C:\Users\user\Desktop\ts.exe MD5: AD57D446C107B5ABD83B6180456CD0DD)
  - conhost.exe (PID: 4724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
ts.exe	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
ts.exe	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0xa7cfe:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xaa853:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xab94f:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xb218d:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xa6601:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0xb1a8c:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0xaa841:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xab93d:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xab3a7:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0xb3d19:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0xa6272:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0xa6615:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0xa3097:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\62366813.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
C:\Users\user\Desktop\62366813.dll	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x92ea:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xbe3f:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcf3b:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x13779:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x7bed:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x13078:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0xbe2d:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcf29:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc993:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x15305:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x785e:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x7c01:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0x4683:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.562441647.00007FFA0AED1000.00000020.00000001.01000000.00000004.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.562441647.00007FFA0AED1000.00000020.00000001.01000000.00000004.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x8eea:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xba3f:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcb3b:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x13379:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x77ed:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x12c78:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0xba2d:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcb29:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc593:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x14f05:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x745e:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x7801:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0x4283:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
00000000.00000003.299862162.00000228231C0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000003.299862162.00000228231C0000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x92ea:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xbe3f:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcf3b:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x13779:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x7bed:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x13078:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0xbe2d:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xcf29:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc993:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x15305:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x785e:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x7c01:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0x4683:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
00000000.00000003.299383409.0000022823350000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.ts.exe.228231c0000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
0.3.ts.exe.228231c0000.3.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x86ea:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xb23f:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc33b:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x12b79:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x6fed:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x12478:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4 C 89 40 18 4C 89 48 20 C3 • 0xb22d:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc329:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xbd93:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x14705:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 4 9 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x6c5e:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x7001:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0x3a83:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
0.3.ts.exe.228233eea14.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.3.ts.exe.228233eea14.0.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x86ea:$chunk_0: 4C 8D 9C 24 B0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xb23f:$chunk_0: 4C 8D 9C 24 00 01 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc33b:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x12b79:$chunk_0: 4C 8D 9C 24 A0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x6fed:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x12478:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4 C 89 40 18 4C 89 48 20 C3 • 0xb22d:$chunk_3: 48 8B 45 27 BB 01 00 00 00 48 89 07 8B 45 2F 89 47 08 4C 8D 9C 24 00 01 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xc329:$chunk_3: 48 8B 45 3F BB 01 00 00 00 48 89 07 8B 45 47 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xbd93:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x14705:$chunk_4: 48 39 3B 4C 8D 9C 24 90 00 00 00 4 9 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x6c5e:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 D0 01 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x7001:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B • 0x3a83:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
0.3.ts.exe.228231c0000.3.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

E-Banking Fraud

Yara detected Emotet

System Summary

Malicious sample detected (through community Yara rule)

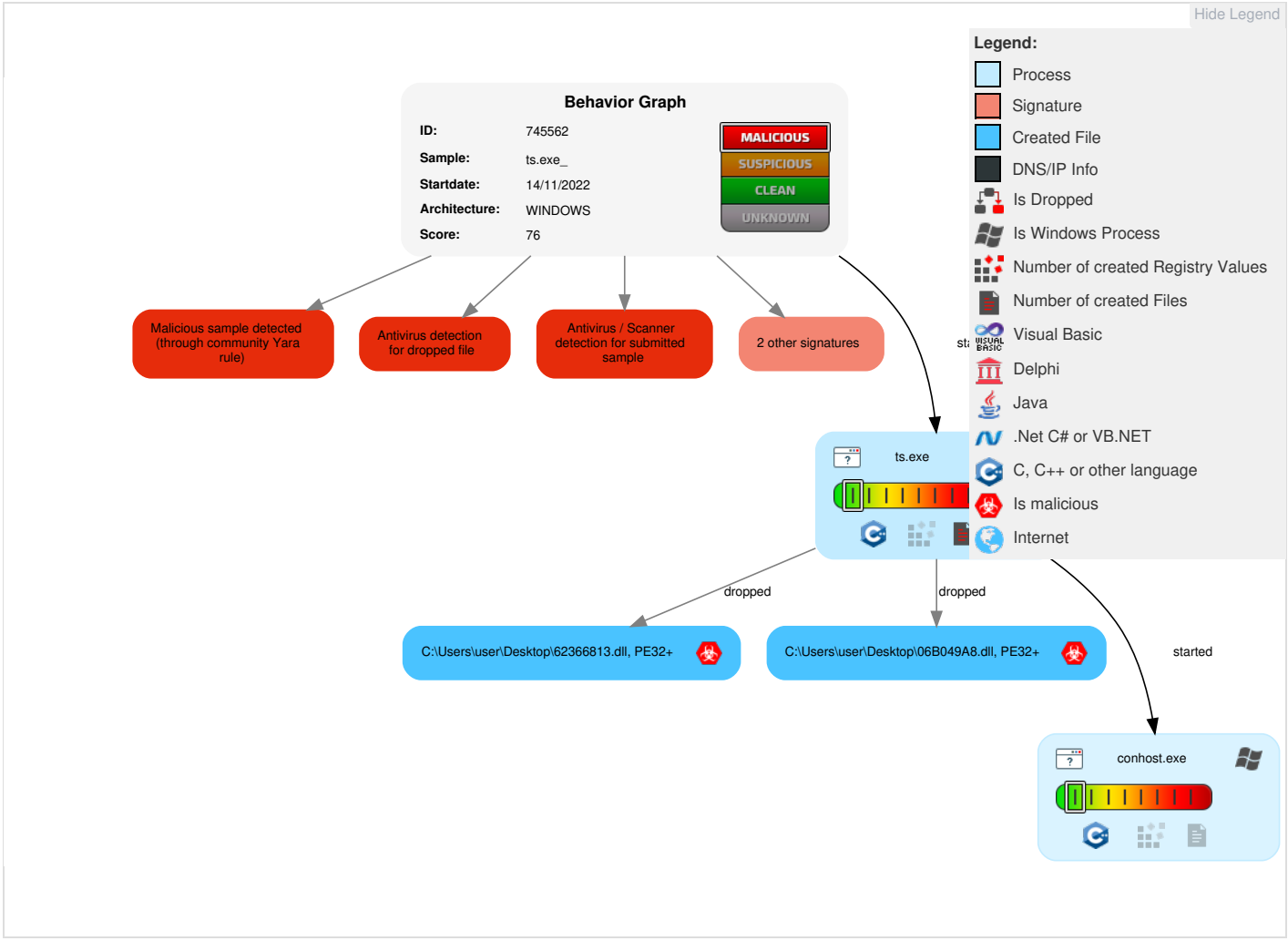
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	2 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	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 File and Directory 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	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

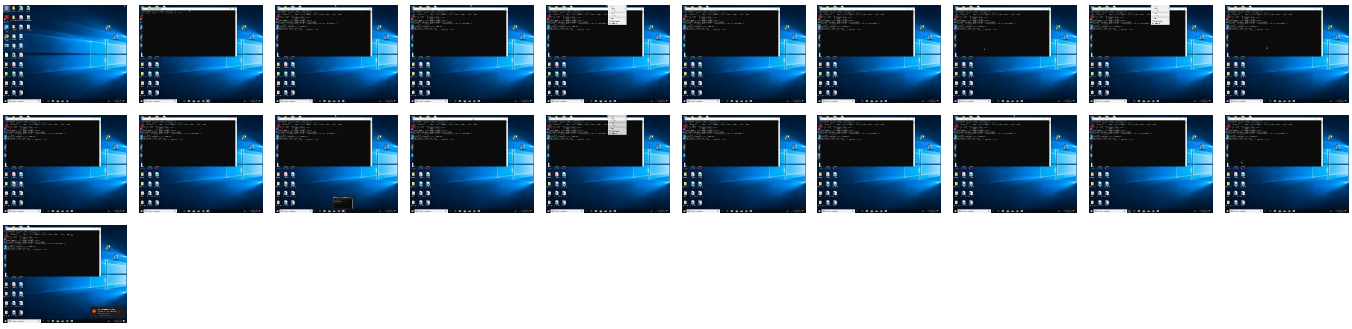
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ts.exe	100%	Avira	HEUR/AGEN.1213146	
ts.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\62366813.dll	100%	Avira	HEUR/AGEN.1251140	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.ts.exe.228231c0000.3.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.3.ts.exe.228233eea14.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.ts.exe.7ffa0aed0000.2.unpack	100%	Avira	HEUR/AGEN.1251140		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	745562
Start date and time:	2022-11-14 14:05:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ts.exe_ (renamed file extension from exe_ to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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:	mal76.troj.winEXE@2/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85% (good quality ratio 77.3%) • Quality average: 62.1% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\06B049A8.dll

Process:	C:\Users\user\Desktop\ts.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	121344
Entropy (8bit):	6.020791170598696
Encrypted:	false
SSDEEP:	3072:dvsJ1yYfWqzIcJ6+R8uQyUtjt8F+8uYW5j:R4cYfWqzr4+R8xZCF+dJ
MD5:	726E5AA7D5929BDC85333E966770FF1A
SHA1:	B43E1A8CF31AD480EC2AE01420E2017488993A8F
SHA-256:	89BE65452EA9DC74134F60311D57B84956D149C600C89801FB152BB04420B16B
SHA-512:	1E69593638B9735C3F7E1E0AE49705B8A10F833D65B9D754973FFF4EDB48DBD270C60E7D157D92F0E42E228C91FCFF2B32D1B1C7F8E4119CA2CBDBBFF70F7FE4
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.q.V.".V.".V."3$.#.V."3$.#eV."3$.#.V."3$.#.V.".V.".V."...#.V."...#.V."...#.V."`/.#.V."`/.#.V."`/1".V."`/.#.V."Rich.V."..... PE..d....&rc....." .....0.....`.....T...d... (..... ..l.....8.....@...@..... ..P.....text..... ..`.rdata..,.... .....@..@.data.....@....pdata.....@..@_RDATA..\.....@..@.rsrc.....@..@.reloc..l.... .....@..B..... .....

C:\Users\user\Desktop\62366813.dll

Process:	C:\Users\user\Desktop\ts.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	95232
Entropy (8bit):	6.655206296626177

Encrypted:	false
SSDEEP:	1536:UTPDxXuEznF2kuaKvu0By22/uTjKd0ovxVg0pJvHj4o0iplGnn5A:UbDx+ELlKtG/u69rj4TiplG5
MD5:	5D182B467B4894159F9A4E956A381B67
SHA1:	0A610C6DE3419CE165D05D770637C8084D584FFD
SHA-256:	ED2239E28A20674D772109DB4F302F7240491FBBC1FB3AD8F30071A6A66736BA
SHA-512:	E6067624F570C40FF0EF2B084F60343379BC83400816217496ACB0897FECB9F4A892CDF4087B27B2E3E58BA0A8873E5CEE6CE8C15B414FC590BE69A6B56B55B4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: C:\Users\user\Desktop\62366813.dll, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: C:\Users\user\Desktop\62366813.dll, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3}!.R.r.R.r.R.r.+.r}S.r.+.r.R.rRich.R.r.....PE..d... 3q`b....." ....\...(.....Y.....`..... t...xZ.....\..... ..`.rdata.....p.....`.....@..@.data.....h.....@....pdata.....l.....@..@..... .....

\Device\ConDrv

Process:	C:\Users\user\Desktop\ts.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	619
Entropy (8bit):	5.332868847941536
Encrypted:	false
SSDEEP:	12:RkjUJY/Ux2UA7FrPHOqF9ptE+7i6x6s+0+5v0aYJ4Cjp5KbJzS+Fo6:mjT/cj2POwTql35vNCp5szS6o6
MD5:	DD2DA9843BF632309924DC6CC54B6DDC
SHA1:	471B4075C9C6D86B94CA1DC43413222F925854FD
SHA-256:	B114B49E322D0D6425F9A555C21BF4C0DEC2E423EE4009BB4B4A099901EAC96C
SHA-512:	FBEFB8EC50D8D879D75D3DFD6399F744D3C72316A425758C13D82DA0992B96B1E9BF951220A0149A010A2B84E10D8FB69CA8C71590ABE172989EF82357C1254
Malicious:	false
Reputation:	low
Preview:	The embedded DLL was dropped to 62366813.dll..Running the embedded DLL with the following parameters:..DLL SHA256:.....ED2239E28A20674D772109DB4F302F7240491FBBC1FB3AD8F30071A6A66736BA..Epoch:.....5..Computer name:....DESKTOPX53HTF9P (random)..Serial:.....7C904961 (random)..Emotet dummy DLL was dropped to 06B049A8.dll..KERNELBASE.dll!BaseUnicodeCommandLine was patched..Command line was patched to "C:\Windows\System32\regsvr32.exe" "06B049A8.dll"..Loading 62366813.dll.....Calling DllEntryPoint() in custom mode.....DllEntryPoint() returned TRUE..The module may still be running in a separated thread..

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	6.442416778819568
TrID:	• Win64 Executable Console (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ts.exe
File size:	744981
MD5:	ad57d446c107b5abd83b6180456cd0dd
SHA1:	8e277fb9bc97bedc7f7f4ba4390cc36702d87b7c
SHA256:	58d9d7c2d4a4140bbdc16c9b6ab1b56244ebc8b1c3eaa1fc63386bbce7acdb4c
SHA512:	35eaa45de9906131f0020640f11eeef46e10244c09c67018a4723cf4932fc3662fbdb61e230f96ce10f47adb12d46e1cf6dc365c79c92c87b1a2679f222a1983
SSDEEP:	12288:LXZ1QgQQ5KLv9Z/QN1MlFuViQic76k0d3hNnC1Pc2lBrxhirous0o3RcYeqzVR8I:LXV2EplBrPZus04p3CBdOj
TLSH:	A8F49E56B2E903F9F5A79134C487560AE7B0784612219B9F47B04AAB1F377726E3F320
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....f.....L.....L.n.....L.....Rich.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x14000b2a8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x637226A2 [Mon Nov 14 11:29:38 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	d02262cfa0ab12b8c838af1a98da369c

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F53C0C9A0ECh
dec eax
add esp, 28h
jmp 00007F53C0C99897h
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
xor ecx, ecx
call dword ptr [00056E53h]
dec eax
mov ecx, ebx
call dword ptr [00056E42h]
call dword ptr [00056E4Ch]
dec eax
mov ecx, eax
mov edx, C0000409h
dec eax
add esp, 20h
pop ebx
dec eax
jmp dword ptr [00056E40h]
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 38h
mov ecx, 00000017h
call dword ptr [00056E34h]
test eax, eax

Instruction
je 00007F53C0C99A29h
mov ecx, 00000002h
int 29h
dec eax
lea ecx, dword ptr [0008F83Ah]
call 00007F53C0C99BEEh
dec eax
mov eax, dword ptr [esp+38h]
dec eax
mov dword ptr [0008F921h], eax
dec eax
lea eax, dword ptr [esp+38h]
dec eax
add eax, 08h
dec eax
mov dword ptr [0008F8B1h], eax
dec eax
mov eax, dword ptr [0008F90Ah]
dec eax
mov dword ptr [0008F77Bh], eax
dec eax
mov eax, dword ptr [esp+40h]
dec eax
mov dword ptr [0008F87Fh], eax
mov dword ptr [0008F755h], C0000409h
mov dword ptr [0008F74Fh], 00000001h
mov dword ptr [0008F759h], 00000001h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a2b4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x288	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x9d000	0x3c9c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa3000	0xd8c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x725a0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x72600	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x72460	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x62000	0x380	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x607b8	0x60800	False	0.4547542908031088	data	6.494863973067288	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x62000	0x18e5e	0x19000	False	0.440009765625	data	5.1869098128532585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7b000	0x214dc	0x1fc00	False	0.48175289124015747	data	5.941625434601615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0x9d000	0x3c9c	0x3e00	False	0.4765625	data	5.653230312289686	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0xa1000	0x15c	0x200	False	0.41796875	data	3.3314562870393805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x288	0x400	False	0.33203125	data	3.8449104178415685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa3000	0xd8c	0xe00	False	0.46791294642857145	data	5.39595888202804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xa2060	0x224	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (488), with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	CryptGetHashParam, CryptDestroyHash, CryptHashData, CryptCreateHash, CryptAcquireContextW, CryptReleaseContext
KERNEL32.dll	ReadFile, VirtualFree, WriteFile, VirtualAlloc, CreateToolhelp32Snapshot, CreateEventW, Sleep, GetLastError, CreateFileA, LoadLibraryA, DeleteFileA, CloseHandle, Module32FirstW, GetFileSize, Module32NextW, GetTickCount, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, SetEvent, ResetEvent, WaitForSingleObjectEx, GetModuleHandleW, GetProcAddress, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, MultiByteToWideChar, WideCharToMultiByte, InitializeCriticalSectionEx, EncodePointer, DecodePointer, GetStringTypeW, LCMapStringEx, GetLocaleInfoEx, CompareStringEx, GetCPInfo, RtlUnwind, RtlUnwindEx, RtlPcToFileHeader, RaiseException, SetLastError, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetCommandLineA, GetCommandLineW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, GetStdHandle, HeapAlloc, HeapFree, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetProcessHeap, SetStdHandle, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, GetTimeZoneInformation, HeapSize, CreateFileW, WriteConsoleW

Possible Origin

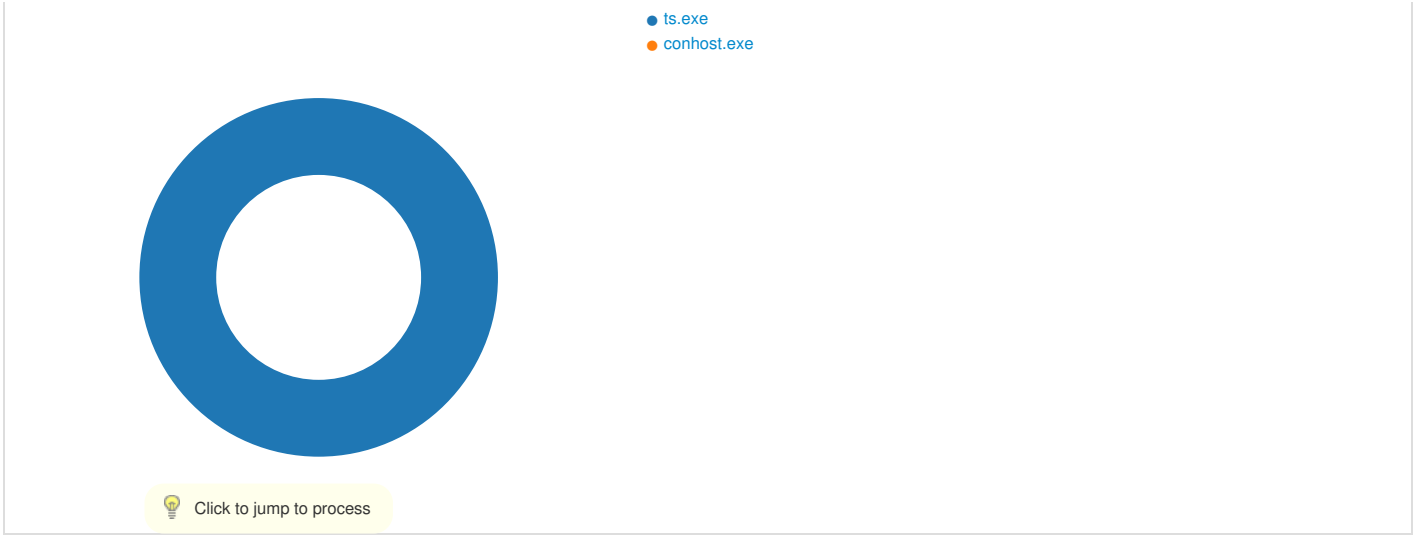
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: ts.exe PID: 3664, Parent PID: 3324

General

Target ID:	0
Start time:	14:06:45
Start date:	14/11/2022
Path:	C:\Users\user\Desktop\ts.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\ts.exe
Imagebase:	0x7ff7a5880000
File size:	744981 bytes
MD5 hash:	AD57D446C107B5ABD83B6180456CD0DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.562441647.00007FFA0AED1000.00000020.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000000.00000002.562441647.00007FFA0AED1000.00000020.00000001.01000000.00000004.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000003.299862162.00000228231C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000000.00000003.299862162.00000228231C0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000003.299383409.0000022823350000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000000.00000003.299383409.0000022823350000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\62366813.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7A58826E4	CreateFileA
C:\Users\user\Desktop\06B049A8.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7A58826E4	CreateFileA
C:\Users\user\AppData\Local\Temp\1B9F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA0AED3632	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1B9F.tmp	success or wait	1	7FFA0AED3953	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\62366813.dll	0	95232	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 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 fd 33 7d 21 fd 52 13 72 fd 52 13 72 fd 52 13 72 fd 2b fd 72 7d 53 13 72 fd 2b fd 72 fd 52 13 72 52 69 63 68 fd 52 13 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 04 00 33 71 60 62 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0c 00 00 5c 01 00 00 28 00 00 00 00 00 00 fd 59 01 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$3}!RrRrRr+r}Sr +rRrRichRrPEd3q`b" \(Y	success or wait	1	7FF7A588270F	WriteFile
\Device\ConDrv	32	32	36 32 33 36 36 38 31 33 2e 64 6c 6c 0d 0a 52 75 6e 6e 69 6e 67 20 74 68 65 20 65 6d 62 65 64 64	62366813.dllRunning the embedd	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	44	12	0d 0a 52 75 6e 6e 69 6e 67 20 74 68	Running th	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	46	2	52 75	Ru	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	103	57	44 4c 4c 20 53 48 41 32 35 36 3a 2e 2e 2e 2e 2e 2e 2e 45 44 32 32 33 39 45 32 38 41 32 30 36 37 34 44 37 37 32 31 30 39 44 42 34 46 33 30 32 46 37 32 34 30 34 39 31 46 42	DLL SHA256:.......ED2239E28A20 674D772109DB4F302F72 40491FB	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	121	18	45 44 32 32 33 39 45 32 38 41 32 30 36 37 34 44 37 37	ED2239E28A20674D77	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	185	64	0d 0a 45 70 6f 63 68 3a 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 35 0d 0a 43 6f 6d 70 75 74 65 72 20 6e 61 6d 65 3a 2e 2e 2e 2e 44 45 53 4b 54 4f 50 58 35 33 48 54 46 39 50 20 28 72 61 6e 64 6f 6d	Epoch:............5Computer na me:....DESKTOPX53HTF 9P (random	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	187	2	45 70	Ep	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	205	18	35 0d 0a 43 6f 6d 70 75 74 65 72 20 6e 61 6d 65 3a 2e	5Computer name:.	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	206	1	0d		success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	208	2	43 6f	Co	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	226	18	44 45 53 4b 54 4f 50 58 35 33 48 54 46 39 50 20 28 72	DESKTOPX53HTF9P (r	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	241	15	20 28 72 61 6e 64 6f 6d 29 0d 0a 53 65 72 69	(random)Seri	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	243	2	72 61	ra	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	249	6	29 0d 0a 53 65 72	)Ser	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	252	3	53 65 72	Ser	success or wait	1	7FF7A58D6ECD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	270	18	37 43 39 30 34 39 36 31 20 28 72 61 6e 64 6f 6d 29 0d	7C904961 (random)	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	278	8	20 28 72 61 6e 64 6f 6d	(random	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	280	2	72 61	ra	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	286	6	29 0d 0a 45 6d 6f	)Emo	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	289	3	45 6d 6f	Emo	success or wait	1	7FF7A58D6ECD	WriteFile
C:\Users\user\Desktop\06B049A8.dll	0	121344	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 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 37 fd 71 fd 56 fd 22 fd 56 fd 22 fd 56 fd 22 33 24 fd 23 fd 56 fd 22 33 24 fd 23 65 56 fd 22 33 24 fd 23 fd 56 fd 22 33 24 fd 23 fd 56 fd 22 fd 56 fd 22 fd 56 fd 22 fd 2e fd 23 fd 56 fd 22 fd 2e fd 23 fd 56 fd 22 fd 2e fd 23 fd 56 fd 22 60 2f fd 23 fd 56 fd 22 60 2f fd 23 fd 56 fd 22 60 2f 31 22 fd 56 fd 22 60 2f fd 23 fd 56 fd 22 52 69 63 68 fd 56 fd 22 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7qV"V"V"3$#V"3$#eV"3$#V"3$#V"V"V".#V".#V".#V "`/#V"`/#V"`/1"V"`/#V"RichV"	success or wait	1	7FF7A588270F	WriteFile
\Device\ConDrv	321	32	30 36 42 30 34 39 41 38 2e 64 6c 6c 0d 0a 4b 45 52 4e 45 4c 42 41 53 45 2e 64 6c 6c 21 42 61 73	06B049A8.dllKERNELBASE.dll!Bas	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	333	12	0d 0a 4b 45 52 4e 45 4c 42 41 53 45	KERNELBASE	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	335	2	4b 45	KE	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	336	1	45	E	success or wait	14	7FF7A58D6ECD	WriteFile
\Device\ConDrv	350	1	42	B	success or wait	36	7FF7A58D6ECD	WriteFile
\Device\ConDrv	387	1	6f	o	success or wait	28	7FF7A58D6ECD	WriteFile
\Device\ConDrv	415	1	43	C	success or wait	49	7FF7A58D6ECD	WriteFile
\Device\ConDrv	465	2	4c 6f	Lo	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	473	8	36 32 33 36 36 38 31 33	62366813	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	485	12	2e 2e 2e 0d 0a 43 61 6c 6c 69 6e 67	...Calling	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	490	5	43 61 6c 6c 69	Calli	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	533	43	44 6c 6c 45 6e 74 72 79 50 6f 69 6e 74 28 29 20 72 65 74 75 72 6e 65 64 20 54 52 55 45 0d 0a 54 68 65 20 6d 6f 64 75 6c 65 20 6d	DllEntryPoint() returned TRUEThe module m	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	564	31	54 68 65 20 6d 6f 64 75 6c 65 20 6d 61 79 20 73 74 69 6c 6c 20 62 65 20 72 75 6e 6e 69 6e 67	The module may still be running	success or wait	1	7FF7A58D6ECD	WriteFile
\Device\ConDrv	619	55	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7A58D6ECD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ts.exe	unknown	744981	success or wait	1	7FF7A58825AA	ReadFile
C:\Users\user\Desktop\62366813.dll	unknown	95232	success or wait	1	7FF7A58825AA	ReadFile

Analysis Process: conhost.exe PID: **4724**, Parent PID: **3664**

General	
Target ID:	1
Start time:	14:06:45
Start date:	14/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly