ID: 478945
Sample Name: RpDMpvgd55
Cookbook: default.jbs
Time: 12:44:35
Date: 07/09/2021
Version: 33.0.0 White Diamond

Table of Contents

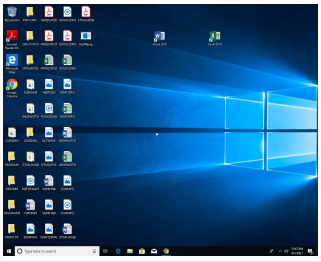
Windows Analysis Report RpDMpvgd55

Overview

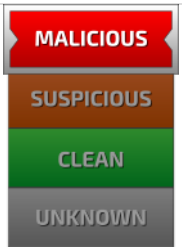
General Information

Sample Name:	RpDMpvgd55 (renamed file extension from none to exe)
Analysis ID:	478945
MD5:	0e569851a5caffd..
SHA1:	32fe45fbef9753d…
SHA256:	8fd4b32e8bc096e.
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



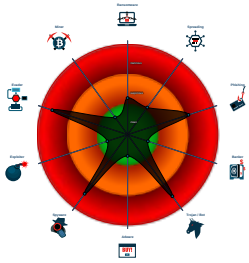
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- RpDMpvgd55.exe (PID: 6900 cmdline: 'C:\Users\user\Desktop\RpDMpvgd55.exe' MD5: 0E569851A5CAFFD0924437714DB46ABE)
  - cmd.exe (PID: 7156 cmdline: 'C:\Windows\System32\cmd.exe' /c copy 'C:\Users\user\Desktop\RpDMpvgd55.exe' 'C:\Users\user\AppData\Local\start.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 2896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - explorer.exe (PID: 5632 cmdline: 'C:\Windows\System32\explorer.exe' /c, 'C:\Users\user\AppData\Local\start.exe' MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 6380 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - start.exe (PID: 6344 cmdline: 'C:\Users\user\AppData\Local\start.exe' MD5: 0E569851A5CAFFD0924437714DB46ABE)
    - start.exe (PID: 1724 cmdline: C:\Users\user\AppData\Local\start.exe MD5: 0E569851A5CAFFD0924437714DB46ABE)
      - vbc.exe (PID: 7032 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp8598.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - vbc.exe (PID: 1768 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp7DB4.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- start.exe (PID: 3940 cmdline: 'C:\Users\user\AppData\Local\start.exe' -boot MD5: 0E569851A5CAFFD0924437714DB46ABE)
  - start.exe (PID: 4928 cmdline: C:\Users\user\AppData\Local\start.exe MD5: 0E569851A5CAFFD0924437714DB46ABE)
    - vbc.exe (PID: 6728 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpD4F0.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- start.exe (PID: 6988 cmdline: 'C:\Users\user\AppData\Local\start.exe' -boot MD5: 0E569851A5CAFFD0924437714DB46ABE)
  - start.exe (PID: 6428 cmdline: C:\Users\user\AppData\Local\start.exe MD5: 0E569851A5CAFFD0924437714DB46ABE)
    - vbc.exe (PID: 2232 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpFEB0.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.611611100.00000000026C3000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000017.00000002.611611100.00000000026C3000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000017.00000002.608775895.0000000000522000.00000040.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x878fa:$s1: HawkEye Keylogger • 0x87963:$s1: HawkEye Keylogger • 0x80d3d:$s2: _ScreenshotLogger • 0x80d0a:$s3: _PasswordStealer
00000017.00000002.608775895.0000000000522000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000000B.00000002.611844683.0000000002743000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x78ab9:$s2: _ScreenshotLogger • 0x79005:$s2: _ScreenshotLogger • 0x78a86:$s3: _PasswordStealer • 0x78fd2:$s3: _PasswordStealer
Click to see the 71 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.3.start.exe.3d75810.2.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x696fa:$a1: logins.json • 0x6965a:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encrypteduUsername, encryptedPassword FROM moz_login • 0x69e7e:$s4: \mozsqlite3.dll • 0x686ee:$s5: SMTP Password
19.3.start.exe.3d75810.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
19.3.start.exe.3d75810.2.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
13.2.start.exe.4bc23e0.4.unpack	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x85cfa:$s1: HawkEye Keylogger • 0x85d63:$s1: HawkEye Keylogger • 0x7f13d:$s2: _ScreenshotLogger • 0x7f10a:$s3: _PasswordStealer
13.2.start.exe.4bc23e0.4.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x856cd:$name: ConfuserEx • 0x843da:$compile: AssemblyTitle
Click to see the 215 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

System Summary:

Malicious sample detected (through community Yara rule)

PE file has nameless sections

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Yara detected WebBrowserPassView password recovery tool

Tries to steal Mail credentials (via file access)

Tries to steal Instant Messenger accounts or passwords

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

Remote Access Functionality:

Yara detected HawkEye Keylogger

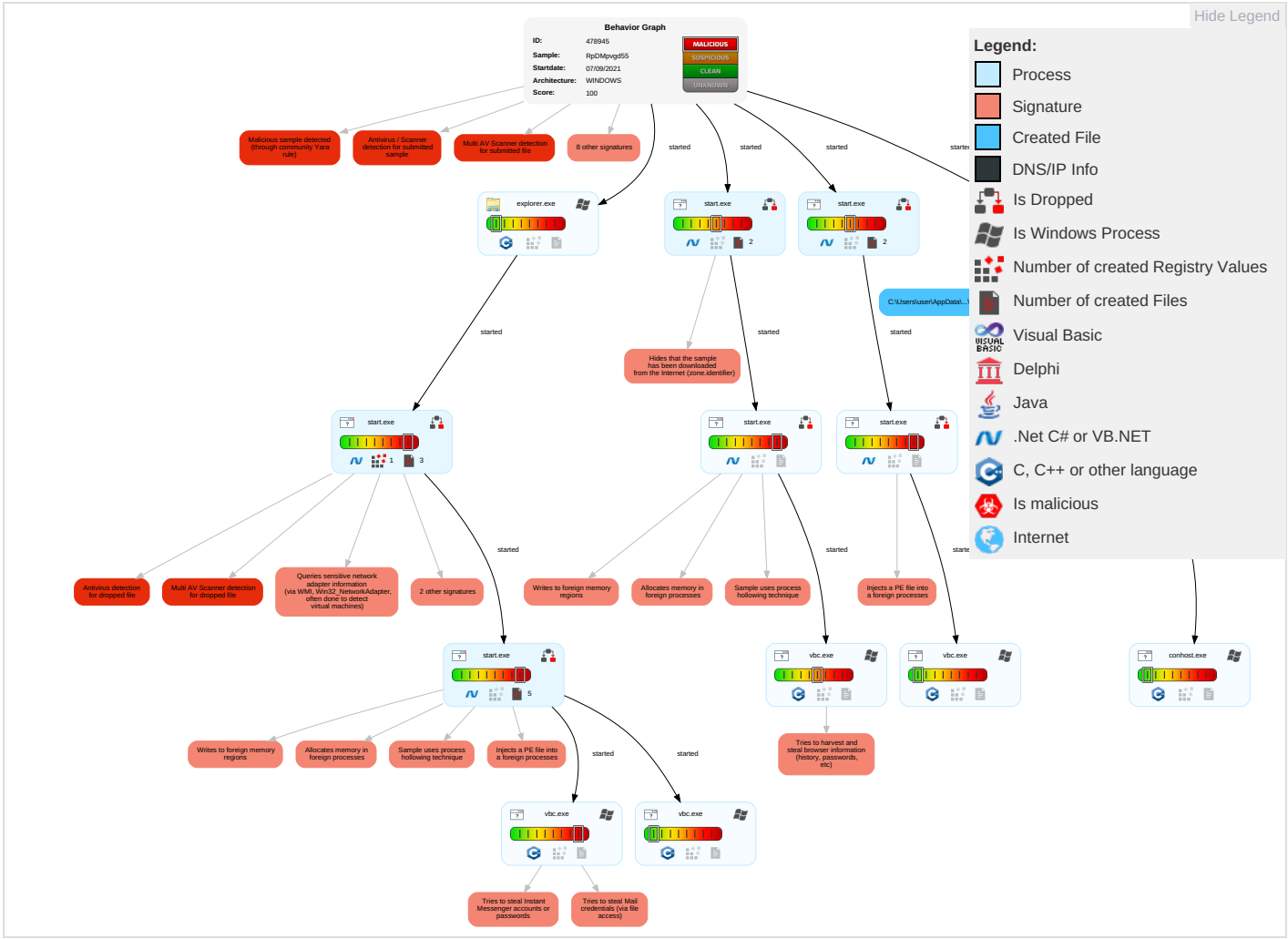
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Registry Run Keys / Startup Folder 1	Process Injection 4 1 1	Disable or Modify Tools 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Remote Acce Software 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials In Files 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganograph
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 4	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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
RpDMpvgd55.exe	72%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
RpDMpvgd55.exe	100%	Avira	HEUR/AGEN.1101677	
RpDMpvgd55.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\start.exe	100%	Avira	HEUR/AGEN.1101677	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\start.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\start.exe	72%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.start.exe.2a0000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
23.2.start.exe.90000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
11.0.start.exe.2a0000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
25.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
11.2.start.exe.730000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.start.exe.b40000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
23.0.start.exe.90000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
23.2.start.exe.520000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.2.RpDMpvgd55.exe.c30000.0.unpack	100%	Avira	TR/Crypt.XDR.Gen		Download File
19.2.start.exe.500000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.2.start.exe.60000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
28.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.0.RpDMpvgd55.exe.c30000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
19.0.start.exe.60000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
13.2.start.exe.8c0000.0.unpack	100%	Avira	TR/Crypt.XDR.Gen		Download File
9.2.start.exe.e50000.0.unpack	100%	Avira	TR/Crypt.XDR.Gen		Download File
13.0.start.exe.8c0000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
18.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
9.0.start.exe.e50000.0.unpack	100%	Avira	HEUR/AGEN.1101677		Download File
17.2.start.exe.b40000.0.unpack	100%	Avira	TR/Crypt.XDR.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	URL Reputation	safe	
http://pomf.cat/upload.phpCContent-Disposition:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	478945
Start date:	07.09.2021
Start time:	12:44:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RpDMpvgd55 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@25/10@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 31.8% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:45:41	API Interceptor	1x Sleep call for process: RpDMpvgd55.exe modified
12:45:56	API Interceptor	6x Sleep call for process: start.exe modified
12:45:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Application C:\Users\user\AppData\Local\start.exe -boot
12:46:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Application C:\Users\user\AppData\Local\start.exe -boot

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RpDMpvgd55.exe.log	
Process:	C:\Users\user\Desktop\RpDMpvgd55.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.347708444648342
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKe:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9p7
MD5:	A4FC14375EBDDC11779CC066BB3E1E83
SHA1:	3A0692B02588ED06D0E35A6DE2686450E1398F70
SHA-256:	273BA80AF3E6DE87E26C0C5C3DEEC70707AF4DAF8C68D8E35E05D19FBC580F40
SHA-512:	EA313CA134E20208052BEDE1EA1E10A392C4A5251673556DEF47786580620D4270412391F1C2030372FEF1F5F0A006E41C8FCE25CD22C8BEE91173BD84E64B76
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\start.exe.log	
Process:	C:\Users\user\AppData\Local\start.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21q1KDLI4M9XKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9px
MD5:	3A72FBECA73A61C00EECBDEC37EAD411
SHA1:	E2330F7B3182A857BB477B2492DDECC2A8488211
SHA-256:	2D4310C4AB9ADEFD6169137CD8973D23D779EDD968B8B39DBC072BF888D0802C
SHA-512:	260EBFB3045513A0BA14751A6B67C95CDA83DD122DC8510EF89C9C42C19F076C8C40645E0795C15ADDF57DB65513DD73EB3C5D0C883C6FB1C34165BE35AE38 9
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\24b52983-2844-023d-2e9c-886bda31e7b2	
Process:	C:\Users\user\AppData\Local\start.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.140319531114783
Encrypted:	false
SSDEEP:	3:ByXTBQuyNs+AX8VVf3PWbfcn:BENNYV1/mcn
MD5:	3FFDA9E87C97BF334CACDFB5FEF216EA
SHA1:	1BA32A69058FFAE9841398A8FD9D279D206E5329
SHA-256:	9A9F19A828A6A8057606E972A8442474E48CF15344EBE4B812803C0B80EC56C5
SHA-512:	DC3A182A593F1ED8E64009C4CD4A347A75A35156D45D0579AD5ED33D830D3BE8F84A7521782DA324E7203BAC047CCEDBEFEAA8EBE35146C2F4FCD06871E32 C8
Malicious:	false

C:\Users\user\AppData\Local\Temp\24b52983-2844-023d-2e9c-886bda31e7b2	
Reputation:	unknown
Preview:	6k/eK3YS2T0duwnxblQTuhY229ghIfQq6TezeFSidSeCNd0zrWqjsdo/nnmEHac9

C:\Users\user\AppData\Local\Temp\bhv25CB.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xf9eae11b, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.8910213227408189
Encrypted:	false
SSDEEP:	24576:1h+wP17f2sZiPHihgmKdTnjVccgeTaNX:WsZqT
MD5:	9B9566F47E2B75CEECFF5A7577BDF696
SHA1:	83015F3A06D1989AAB2C17D5A13F070100A2828E
SHA-256:	DDEA12ED30FECAD827BAD3435DA24159A6677A750B22ABEAB6CE02741371C82C
SHA-512:	66DF3D2397E773080F2F10FBF3B785312883B4205F60E0BDAA7751D0A094147C0B0C8ADF083C8AB451CD9E66250B46809AE61355CE0D8063B46BA48B50FB46B5
Malicious:	false
Reputation:	unknown
Preview:	....p.....Ef..4...w.....%.....-...y...-...y..h.'.....W.4...w.....[.....B..... ....-...y?..... .....o.PA.....y?{.....R1.....y?..... .....

C:\Users\user\AppData\Local\Temp\bhvADAD.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xf9eae11b, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.8976801204988787
Encrypted:	false
SSDEEP:	24576:1h+wP17f2sZiPHihgmKdTnjVccgeTaNX:WsZqT
MD5:	A19B45FCC96F3F2111D19E5F65BE60ED
SHA1:	E46224300E786AC6AF282474E079123C0F3C3E85
SHA-256:	6730E0916072F37F86DFC2416827C0E59BC0B6F0DD263C8524B7859034C59500
SHA-512:	07B247D21B76F3686213CB1CC556BE433DB47E0217105B373F29130011739D8A9A4622E4DCB659DB1149B95E1BB962E060B94C299103A16BD300FB1514882CAF
Malicious:	false
Reputation:	unknown
Preview:	....p.....Ef..4...w.....%.....-...y...-...y..h.'.....W.4...w.....[.....B..... ....-...y?..... .....o.PA.....y?{.....R1.....y?..... .....

C:\Users\user\AppData\Local\Temp\bhvFBFC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xf9eae11b, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.8910213227408189
Encrypted:	false
SSDEEP:	
MD5:	9B9566F47E2B75CEECFF5A7577BDF696
SHA1:	83015F3A06D1989AAB2C17D5A13F070100A2828E
SHA-256:	DDEA12ED30FECAD827BAD3435DA24159A6677A750B22ABEAB6CE02741371C82C
SHA-512:	66DF3D2397E773080F2F10FBF3B785312883B4205F60E0BDAA7751D0A094147C0B0C8ADF083C8AB451CD9E66250B46809AE61355CE0D8063B46BA48B50FB46B5
Malicious:	false
Reputation:	unknown
Preview:	....p.....Ef..4...w.....%.....-...y...-...y..h.'.....W.4...w.....[.....B..... ....-...y?..... .....o.PA.....y?{.....R1.....y?..... .....

C:\Users\user\AppData\Local\Temp\tmp8598.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp8598.tmp	
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\Temp\tmpD4F0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\Temp\tmpFEB0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\start.exe	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	791552
Entropy (8bit):	**7.993194071005919**
Encrypted:	**true**
SSDEEP:	
MD5:	0E569851A5CAFFD0924437714DB46ABE
SHA1:	32FE45FBEF9753D08978AD11A0001B29F032BA34
SHA-256:	8FD4B32E8BC096E4F4C34BA302295CAA4ACCD453EDFF3E4A153397710FBC4A94
SHA-512:	0229B9515E0BD71D7C4B2E5BC6A30DBA5B69BA761BF20A1C4A32D112D563E758284B74FF067E0815DD8207DADD40D60292AD0D7998AA501017944949E32AE7A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 72%

C:\Users\user\AppData\Local\start.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...*..H.....R..... ....@.. ....@.....W....@.....`.....H.....lUh.FD.|.... .....@....text....O.....P..... ..`.rsr c.....@.....@..@.reloc.....`.....@..B..... ..`..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.993194071005919
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	RpDMpvgd55.exe
File size:	791552
MD5:	0e569851a5caffd0924437714db46abe
SHA1:	32fe45fbef9753d08978ad11a0001b29f032ba34
SHA256:	8fd4b32e8bc096e4f4c34ba302295caa4accd453edff3e4a153397710fbc4a94
SHA512:	0229b9515e0bd71d7c4b2e5bc6a30dba5b69ba761bf20a1c4a32d112d563e758284b74ff067e0815dd8207dadd40c60292ad0d7998aa501017944949e32ae7a0
SSDEEP:	12288:8TGAG62AIMjAqahuv4riAdbaMiwIRIRP4IPIB65UM4SD7YQyV4TciTlCD3Ha9N:8TI62AS75aMiwiq4IPIBvMbGdi+qP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...*..H.....R..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c800a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x48960B2A [Sun Aug 3 19:46:50 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
lUhFD	0x2000	0xbb27c	0xbb400	False	1.00014602804	data	7.99971985547	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xbe000	0x4fc0	0x5000	False	0.726708984375	data	6.79648993685	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x610	0x800	False	0.34326171875	data	3.53237877786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.09262353601	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xc8000	0x10	0x200	False	0.044921875	dBase III DBT, version number 0, next free block index 779296	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RpDMpvgd55.exe PID: 6900 Parent PID: 528

General

Start time:	12:45:32
Start date:	07/09/2021
Path:	C:\Users\user\Desktop\RpDMpvgd55.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RpDMpvgd55.exe'
Imagebase:	0xc30000

File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.370358724.0000000004DC8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.370358724.0000000004DC8000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.368874636.00000000049D6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.368874636.00000000049D6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 7156 Parent PID: 6900

General

Start time:	12:45:39
Start date:	07/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c copy 'C:\Users\user\Desktop\RpDMpvgd55.exe' 'C:\Users\user\AppData\Local\start.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 2896 Parent PID: 7156

General

Start time:	12:45:40
Start date:	07/09/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 5632 Parent PID: 6900

General

Start time:	12:45:42
Start date:	07/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\explorer.exe' /c, 'C:\Users\user\AppData\Local\start.exe'
Imagebase:	0x8b0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 6380 Parent PID: 792

General

Start time:	12:45:44
Start date:	07/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: start.exe PID: 6344 Parent PID: 6380

General

Start time:	12:45:45
Start date:	07/09/2021
Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\start.exe'

Imagebase:	0xe50000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000009.00000002.441589720.0000000005018000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.441589720.0000000005018000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000009.00000002.439008892.0000000004C26000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.439008892.0000000004C26000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 72%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: start.exe PID: 1724 Parent PID: 6344

General

Start time:	12:45:58
Start date:	07/09/2021
Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\start.exe
Imagebase:	0x2a0000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000000B.00000002.611844683.0000000002743000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.611844683.0000000002743000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.611844683.0000000002743000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.617396677.0000000003735000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.617396677.0000000003735000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.614686157.000000000284E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000003.428810541.0000000003FA5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000003.428810541.0000000003FA5000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000000B.00000002.608934819.0000000000732000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.608934819.0000000000732000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: start.exe PID: 3940 Parent PID: 3440

General

Start time:	12:46:04
Start date:	07/09/2021
Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\start.exe' -boot
Imagebase:	0x8c0000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000000D.00000002.484936164.0000000004746000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.484936164.0000000004746000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000000D.00000002.486549188.0000000004B38000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.486549188.0000000004B38000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: start.exe PID: 6988 Parent PID: 3440

General

Start time:	12:46:12
Start date:	07/09/2021
Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\start.exe' -boot
Imagebase:	0xb40000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000011.00000002.503262589.0000000004D28000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.503262589.0000000004D28000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000011.00000002.502748889.0000000004936000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.502748889.0000000004936000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: vbc.exe PID: 7032 Parent PID: 1724

General

Start time:	12:46:16
Start date:	07/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp8598.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000012.00000002.450752133.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: start.exe PID: 4928 Parent PID: 3940

General

Start time:	12:46:19
Start date:	07/09/2021
Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\start.exe
Imagebase:	0x60000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.613981984.0000000003505000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000013.00000002.611636873.0000000002582000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.611636873.0000000002582000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000013.00000002.608001079.0000000000502000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.608001079.0000000000502000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.611315160.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.611315160.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000003.473129874.0000000003D75000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000003.473129874.0000000003D75000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: start.exe PID: 6428 Parent PID: 6988

General

Start time:	12:46:28
Start date:	07/09/2021

Path:	C:\Users\user\AppData\Local\start.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\start.exe
Imagebase:	0x90000
File size:	791552 bytes
MD5 hash:	0E569851A5CAFFD0924437714DB46ABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.611611100.00000000026C3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000002.611611100.00000000026C3000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000017.00000002.608775895.0000000000522000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.608775895.0000000000522000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000017.00000002.611953012.0000000002734000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.611953012.0000000002734000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000002.614119011.00000000036B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000003.490802427.0000000003F25000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000003.490802427.0000000003F25000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: vbc.exe PID: 6728 Parent PID: 4928

General

Start time:	12:46:36
Start date:	07/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpD4F0.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000019.00000002.491000117.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 2232 Parent PID: 6428

General

Start time:	12:46:47

Start date:	07/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpFEB0.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.511356001.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 1768 Parent PID: 1724

General

Start time:	12:47:19
Start date:	07/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp7DB4.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000021.00000002.576492139.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.576492139.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis