



ID: 524274
Sample Name: Hpdyv8oO3j.exe
Cookbook: default.jbs
Time: 10:12:40
Date: 18/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Hpdyv8oO3j.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Dropped Files 5
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
HIPS / PFW / Operating System Protection Evasion: 8
Lowering of HIPS / PFW / Operating System Security Settings: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 23
General 23
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 24
Data Directories 24
Sections 24
Resources 24
Imports 24
Version Infos 24
Network Behavior 24
Snort IDS Alerts 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 25
DNS Queries 25
DNS Answers 25

Copyright Joe Security LLC 2021

HTTP Request Dependency Graph 25
HTTP Packets 26
SMTP Packets 26
Code Manipulations 27
Statistics 27
Behavior 27
System Behavior 27
Analysis Process: Hpdyv8oO3j.exe PID: 6436 Parent PID: 6108 27
General 27
File Activities 27
File Created 27
File Written 27
Analysis Process: Keylogger.exe PID: 4492 Parent PID: 6436 27
General 27
File Activities 28
File Created 28
File Written 28
File Read 29
Analysis Process: hhzclipper.exe PID: 1244 Parent PID: 6436 29
General 29
File Activities 29
File Created 29
File Read 29
Analysis Process: RedLine.MainPanel-cracked.exe PID: 4140 Parent PID: 6436 29
General 29
File Activities 30
File Created 30
File Written 30
File Read 30
Registry Activities 30
Key Created 30
Key Value Created 30
Analysis Process: RedLine.MainPanel-cracked.exe PID: 7032 Parent PID: 6436 30
General 30
File Activities 30
File Created 30
File Written 30
File Read 30
Analysis Process: cmd.exe PID: 3348 Parent PID: 6436 31
General 31
File Activities 31
File Read 31
Analysis Process: conhost.exe PID: 6232 Parent PID: 3348 31
General 31
Analysis Process: ViRuS.exe PID: 2988 Parent PID: 6436 31
General 31
File Activities 32
File Created 32
File Written 32
File Read 32
Registry Activities 32
Key Value Created 32
Analysis Process: attrib.exe PID: 5332 Parent PID: 2988 32
General 32
Analysis Process: conhost.exe PID: 5308 Parent PID: 5332 32
General 32
Analysis Process: attrib.exe PID: 7160 Parent PID: 2988 32
General 32
Analysis Process: conhost.exe PID: 7140 Parent PID: 7160 33
General 33
Analysis Process: taskkill.exe PID: 7116 Parent PID: 2988 33
General 33
Analysis Process: conhost.exe PID: 7120 Parent PID: 7116 33
General 33
Analysis Process: RedLine.exe PID: 4236 Parent PID: 4140 34
General 34
Analysis Process: Windows Update.exe PID: 5624 Parent PID: 4492 34
General 34
Analysis Process: user32dll.exe PID: 7128 Parent PID: 3352 36
General 36
Analysis Process: taskkill.exe PID: 7156 Parent PID: 7128 36
General 36
Analysis Process: conhost.exe PID: 7080 Parent PID: 7156 37
General 37
Analysis Process: netsh.exe PID: 7096 Parent PID: 4236 37
General 37
Analysis Process: conhost.exe PID: 6480 Parent PID: 7096 37
General 37
Analysis Process: dw20.exe PID: 4332 Parent PID: 5624 38
General 38
Analysis Process: vbc.exe PID: 6444 Parent PID: 5624 38
General 38
Analysis Process: vbc.exe PID: 1364 Parent PID: 5624 38
General 38
Analysis Process: vbc.exe PID: 1980 Parent PID: 5624 38
General 38
Disassembly 39
Code Analysis 39

Copyright Joe Security LLC 2021

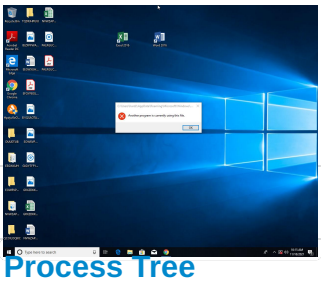
Windows Analysis Report Hpdyv8oO3j.exe

Overview

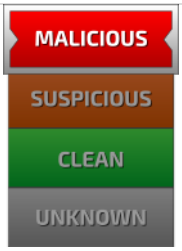
General Information

Sample Name:	Hpdyv8oO3j.exe
Analysis ID:	524274
MD5:	dffaf08a25150b3…
SHA1:	a28b135b64a08d..
SHA256:	8fdbfbf55033187…
Tags:	exe njrat RAT
Infos:	

Most interesting Screenshot:



Detection



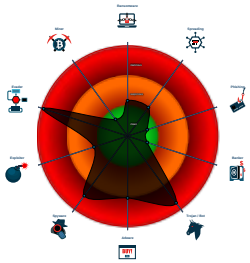
HawkEye
MailPassView
Njrat

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Multi AV Scanner detection for dropp…
- Creates multiple autostart registry ke…
- Uses netsh to modify the Windows n…
- Drops PE files to the startup folder

Classification



Process Tree

- **System is w10x64**
- Hpdyv8oO3j.exe (PID: 6436 cmdline: "C:\Users\user\Desktop\Hpdyv8oO3j.exe" MD5: DFFAF08A25150B38C19210C180862AEB)
  - Keylogger.exe (PID: 4492 cmdline: "C:\Users\user\AppData\Local\Temp\Keylogger.exe" MD5: C4E4A84909D8FF8DD222B8252365985D)
    - Windows Update.exe (PID: 5624 cmdline: "C:\Users\user\AppData\Roaming\Windows Update.exe" MD5: C4E4A84909D8FF8DD222B8252365985D)
      - dw20.exe (PID: 4332 cmdline: dw20.exe -x -s 2528 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - vbc.exe (PID: 6444 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - vbc.exe (PID: 1364 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - vbc.exe (PID: 1980 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - hhzclipper.exe (PID: 1244 cmdline: "C:\Users\user\AppData\Local\Temp\hhzclipper.exe" MD5: FC07BE5E90A1FFA22B22D3BC58A43E58)
  - RedLine.MainPanel-cracked.exe (PID: 4140 cmdline: "C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe" MD5: 098F7F40BACA320377ECA83FBF87F534)
    - RedLine.exe (PID: 4236 cmdline: "C:\Users\user\AppData\Roaming\RedLine.exe" MD5: 098F7F40BACA320377ECA83FBF87F534)
      - netsh.exe (PID: 7096 cmdline: netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\RedLine.exe" "RedLine.exe" ENABLE MD5: 98CC37BBF363A38834253E22C80A8F32)
        - conhost.exe (PID: 6480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RedLine.MainPanel-cracked.exe (PID: 7032 cmdline: "C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe" MD5: 098F7F40BACA320377ECA83FBF87F534)
  - cmd.exe (PID: 3348 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\HOST.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ViRuS.exe (PID: 2988 cmdline: "C:\Users\user\AppData\Local\Temp\ViRuS.exe" MD5: D0F09063EA6922ACBFC734145FA48203)
    - attrib.exe (PID: 5332 cmdline: C:\Windows\System32\attrib.exe" +r +h +s +a "C:\Windows\system32\user32dll.exe MD5: A5540E9F87D4CB083BDF8269DEC1CFF9)
      - conhost.exe (PID: 5308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - attrib.exe (PID: 7160 cmdline: C:\Windows\System32\attrib.exe" +r +h +s +a "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\explorer.lnk MD5: A5540E9F87D4CB083BDF8269DEC1CFF9)
      - conhost.exe (PID: 7140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 7116 cmdline: taskkill /f /im "ViRuS.exe" MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
      - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- user32dll.exe (PID: 7128 cmdline: "C:\Windows\SysWOW64\user32dll.exe" MD5: D0F09063EA6922ACBFC734145FA48203)
  - taskkill.exe (PID: 7156 cmdline: taskkill /f /im "user32dll.exe" MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - WerFault.exe (PID: 1008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7156 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- RedLine.exe (PID: 6688 cmdline: "C:\Users\user\AppData\Roaming\RedLine.exe" .. MD5: 098F7F40BACA320377ECA83FBF87F534)
- WindowsUpdate.exe (PID: 6300 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: C4E4A84909D8FF8DD222B8252365985D)
  - Windows Update.exe (PID: 5248 cmdline: "C:\Users\user\AppData\Roaming\Windows Update.exe" MD5: C4E4A84909D8FF8DD222B8252365985D)
    - dw20.exe (PID: 7048 cmdline: dw20.exe -x -s 2472 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
    - vbc.exe (PID: 4964 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 7156 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
- RedLine.exe (PID: 4864 cmdline: "C:\Users\user\AppData\Roaming\RedLine.exe" .. MD5: 098F7F40BACA320377ECA83FBF87F534)
- WindowsUpdate.exe (PID: 4456 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: C4E4A84909D8FF8DD222B8252365985D)
- RedLine.exe (PID: 3408 cmdline: "C:\Users\user\AppData\Roaming\RedLine.exe" .. MD5: 098F7F40BACA320377ECA83FBF87F534)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Keylogger.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	0x7b809:$key: HawkEyeKeylogger 0x7db3f:$salt: 099u787978786 0x7bec6:$string1: HawkEye_Keylogger 0x7cd19:$string1: HawkEye_Keylogger 0x7da9f:$string1: HawkEye_Keylogger 0x7c2af:$string2: holdermail.txt 0x7c2cf:$string2: holdermail.txt 0x7c1f1:$string3: wallet.dat 0x7c209:$string3: wallet.dat 0x7c21f:$string3: wallet.dat 0x7d663:$string4: Keylog Records 0x7d97b:$string4: Keylog Records 0x7db97:$string5: do not script --> 0x7b7f1:$string6: \pidloc.txt 0x7b87f:$string7: BSPLIT 0x7b88f:$string7: BSPLIT

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Keylogger.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
C:\Users\user\AppData\Local\Temp\Keylogger.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
C:\Users\user\AppData\Local\Temp\Keylogger.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
C:\Users\user\AppData\Local\Temp\Keylogger.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 13 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.401046205.000000000384C000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000001C.00000000.394707935.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000019.00000002.567099655.000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0000002A.00000002.490818765.0000000002EA1000.00000004.00000001.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0000002A.00000002.490818765.0000000002EA1000.00000004.00000001.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x1e963:$a1: netsh firewall add allowedprogram • 0x341bb:$a1: netsh firewall add allowedprogram • 0x3c1d3:$a1: netsh firewall add allowedprogram • 0x1e933:$a2: SEE_MASK_NOZONECHECKS • 0x3418b:$a2: SEE_MASK_NOZONECHECKS • 0x3c1a3:$a2: SEE_MASK_NOZONECHECKS • 0x1eb53:$b1: [TAP] • 0x343ab:$b1: [TAP] • 0x3c3c3:$b1: [TAP] • 0x1ea4f:$c3: cmd.exe /c ping • 0x342a7:$c3: cmd.exe /c ping • 0x3c2bf:$c3: cmd.exe /c ping
Click to see the 161 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.Windows Update.exe.350b42c.5.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
17.2.Windows Update.exe.7f20000.9.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
4.2.RedLine.MainPanel-cracked.exe.2ad9310.4.raw.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
4.2.RedLine.MainPanel-cracked.exe.2ad9310.4.raw.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x67d3:$a1: netsh firewall add allowedprogram • 0x1c02b:$a1: netsh firewall add allowedprogram • 0x24043:$a1: netsh firewall add allowedprogram • 0x67a3:$a2: SEE_MASK_NOZONECHECKS • 0x1bffb:$a2: SEE_MASK_NOZONECHECKS • 0x24013:$a2: SEE_MASK_NOZONECHECKS • 0x69c3:$b1: [TAP] • 0x1c21b:$b1: [TAP] • 0x24233:$b1: [TAP] • 0x68bf:$c3: cmd.exe /c ping • 0x1c117:$c3: cmd.exe /c ping • 0x2412f:$c3: cmd.exe /c ping
4.2.RedLine.MainPanel-cracked.exe.2ad9310.4.raw.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x67a3:$reg: SEE_MASK_NOZONECHECKS • 0x1bffb:$reg: SEE_MASK_NOZONECHECKS • 0x24013:$reg: SEE_MASK_NOZONECHECKS • 0x64a4:$msg: Execute ERROR • 0x653e:$msg: Execute ERROR • 0x1bcfc:$msg: Execute ERROR • 0x1bd96:$msg: Execute ERROR • 0x23d14:$msg: Execute ERROR • 0x23dae:$msg: Execute ERROR • 0x68bf:$ping: cmd.exe /c ping 0 -n 2 & del • 0x1c117:$ping: cmd.exe /c ping 0 -n 2 & del • 0x2412f:$ping: cmd.exe /c ping 0 -n 2 & del
Click to see the 253 entries				

Sigma Overview

System Summary:



Sigma detected: Netsh Port or Application Allowed

Sigma detected: Hiding Files with Attrib.exe

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:



May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected HawkEye Keylogger

Installs a global keyboard hook

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:



Yara detected Njrat

System Summary:



Malicious sample detected (through community Yara rule)

Creates files with lurking names (e.g. Crack.exe)

.NET source code contains very large strings

Data Obfuscation:



.NET source code contains potential unpacker

Persistence and Installation Behavior:



Uses cmd line tools excessively to alter registry or file data

Drops executables to the windows directory (C:\Windows) and starts them

Copyright Joe Security LLC 2021

Boot Survival:



- Creates multiple autostart registry keys
- Drops PE files to the startup folder
- Creates autostart registry keys with suspicious names

Hooking and other Techniques for Hiding and Protection:



- Changes the view of files in windows explorer (hidden files and folders)

HIPS / PFW / Operating System Protection Evasion:



- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Sample uses process hollowing technique
- Writes to foreign memory regions
- .NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:



- Uses netsh to modify the Windows network and firewall settings
- Modifies the windows firewall

Stealing of Sensitive Information:



- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Yara detected Njrat
- Tries to harvest and steal browser information (history, passwords, etc)
- Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:



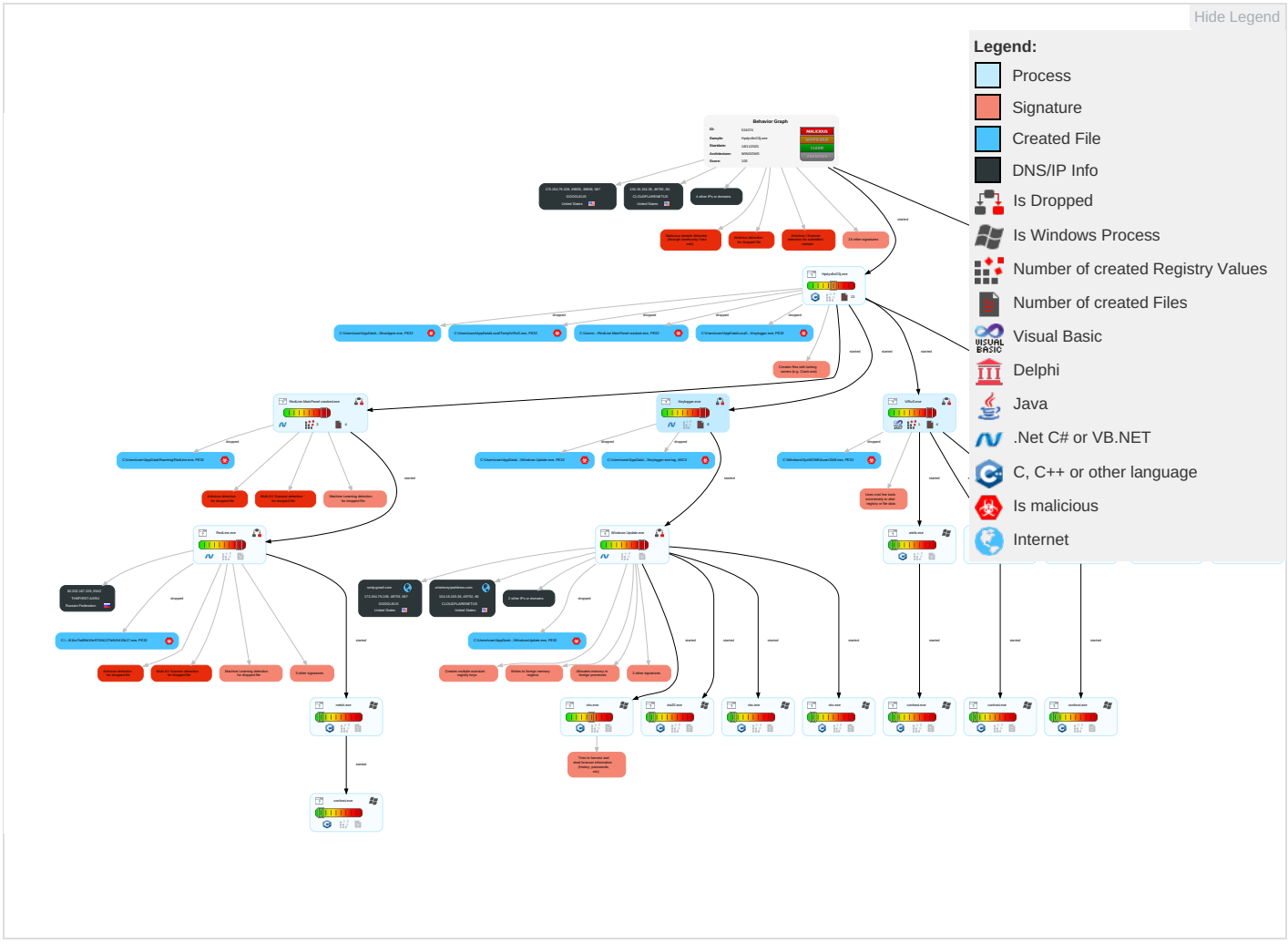
- Yara detected HawkEye Keylogger
- Yara detected Njrat
- Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Ov Network Medi
Default Accounts	Scripting 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Ov Bluetooth
Domain Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Scripting 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 2 1 1	Automated Ex
Local Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 3 2 1	Access Token Manipulation 1	Obfuscated Files or Information 3 1	NTDS	System Information Discovery 1 8	Distributed Component Object Model	Clipboard Data 2	Scheduled Tra

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Command and Scripting Interpreter 1	Network Logon Script	Process Injection 4 1 2	Software Packing 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Limits
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 3 2 1	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 1 7 1	VNC	GUI Input Capture	Exfiltration Ov Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2 2 1	DCSync	Virtualization/Sandbox Evasion 5 1	Windows Remote Management	Web Portal Capture	Exfiltration Ov Alternative Pro
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 5 1	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Ov Symmetric En Non-C2 Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Ov Asymmetric Er Non-C2 Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 4 1 2	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Ov Unencrypted/C Non-C2 Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	System Network Configuration Discovery 1 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Ov Physical Medi

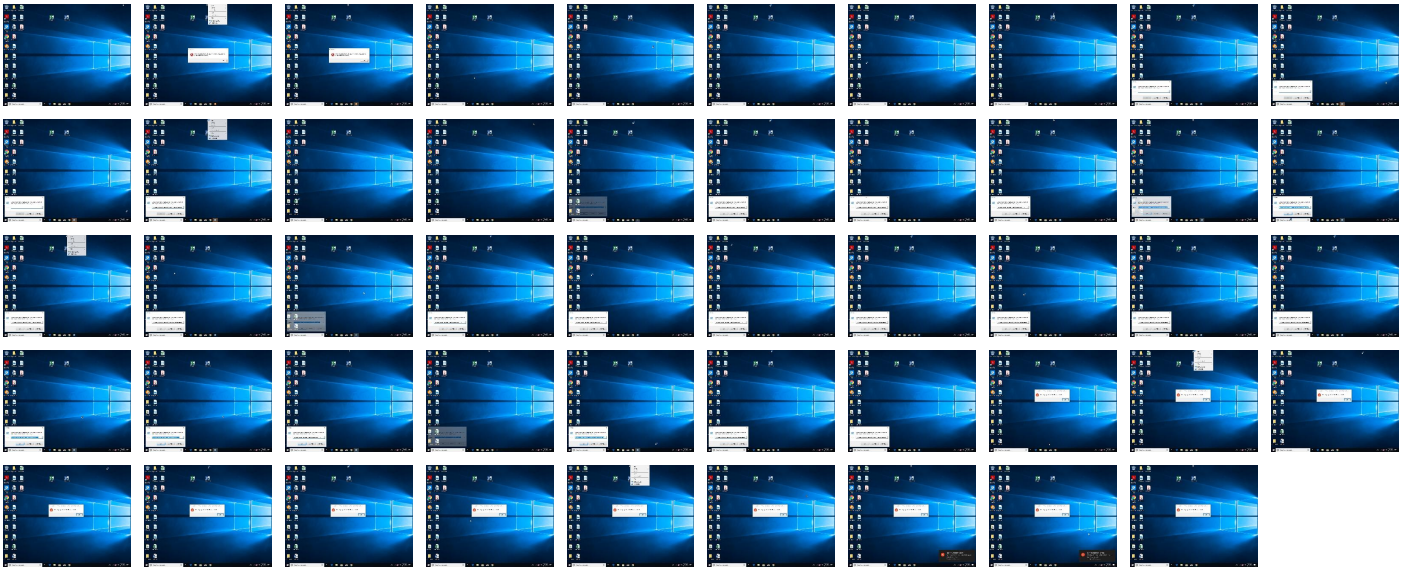
Behavior Graph



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
Hpdyv8oO3j.exe	74%	Metadefender		Browse
Hpdyv8oO3j.exe	100%	ReversingLabs	Win32.Trojan.VBinder	
Hpdyv8oO3j.exe	100%	Avira	HEUR/AGEN.1114177	
Hpdyv8oO3j.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ViRuS.exe	100%	Avira	TR/Agent.32768.2190	
C:\Windows\SysWOW64\user32dll.exe	100%	Avira	TR/Agent.32768.2190	
C:\Users\user\AppData\Roaming\RedLine.exe	100%	Avira	BDS/Bladabindi.ajooc	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\61bc7bd88d10e97264127fe545415b17.exe	100%	Avira	BDS/Bladabindi.ajooc	
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\Keylogger.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Local\Temp\Keylogger.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\hhzclipper.exe	100%	Avira	HEUR/AGEN.1134703	
C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe	100%	Avira	BDS/Bladabindi.ajooc	
C:\Users\user\AppData\Local\Temp\ViRuS.exe	100%	Joe Sandbox ML		
C:\Windows\SysWOW64\user32dll.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\RedLine.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\61bc7bd88d10e97264127fe545415b17.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Keylogger.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\hhzclipper.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.Ratenjay	
C:\Users\user\AppData\Local\Temp\ViRuS.exe	83%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ViRuS.exe	93%	ReversingLabs	Win32.Worm.Changeup	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\61bc7bd88d10e97264127fe545415b17.exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.Ratenjay	
C:\Users\user\AppData\Roaming\RedLine.exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.Ratenjay	
C:\Windows\SysWOW64\user32dll.exe	83%	Metadefender		Browse
C:\Windows\SysWOW64\user32dll.exe	93%	ReversingLabs	Win32.Worm.Changeup	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Keylogger.exe.760000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.0.Keylogger.exe.760000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
28.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.0.Hpdyv8oO3j.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140785		Download File
28.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.Hpdyv8oO3j.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140785		Download File
19.0.user32dll.exe.400000.0.unpack	100%	Avira	TR/Agent.32768.2190		Download File
17.0.Windows Update.exe.d40000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
17.0.Windows Update.exe.d40000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
19.2.user32dll.exe.400000.0.unpack	100%	Avira	TR/Agent.32768.2190		Download File
17.2.Windows Update.exe.d40000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
17.2.Windows Update.exe.d40000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.2.RedLine.exe.580000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
28.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
4.2.RedLine.MainPanel-cracked.exe.2b3af40.5.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
17.0.Windows Update.exe.d40000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
17.0.Windows Update.exe.d40000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.2.hhzclipper.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1134703		Download File
28.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
28.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
5.0.RedLine.MainPanel-cracked.exe.340000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
0.3.Hpdyv8oO3j.exe.708218.1.unpack	100%	Avira	TR/Agent.32768.2190		Download File
4.0.RedLine.MainPanel-cracked.exe.550000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
28.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.Windows Update.exe.d40000.12.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
17.0.Windows Update.exe.d40000.12.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.0.hhzclipper.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1134703		Download File
4.2.RedLine.MainPanel-cracked.exe.550000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
2.2.Keylogger.exe.760000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.Keylogger.exe.760000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.2.RedLine.MainPanel-cracked.exe.340000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
17.0.Windows Update.exe.d40000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
17.0.Windows Update.exe.d40000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.0.RedLine.exe.580000.0.unpack	100%	Avira	BDS/Bladabindi.ajooc		Download File
8.2.ViRuS.exe.400000.0.unpack	100%	Avira	TR/Agent.32768.2190		Download File
8.0.ViRuS.exe.400000.0.unpack	100%	Avira	TR/Agent.32768.2190		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/moVDfISia2k.crl0	0%	URL Reputation	safe	
http://https://Esteamcommunity.com/tradeoffer/new/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comceu	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856811916691;gt	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnz	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasuq/w	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	URL Reputation	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cna	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnT	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=6856	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
smtp.gmail.com	173.194.79.109	true	false		high
231.58.0.0.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.154.36	unknown	United States		13335	CLOUDFLARENETUS	false
173.194.79.108	unknown	United States		15169	GOOGLEUS	false
173.194.79.109	smtp.gmail.com	United States		15169	GOOGLEUS	false
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
82.202.167.226	unknown	Russian Federation		29182	THEFIRST-ASRU	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	524274
Start date:	18.11.2021
Start time:	10:12:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hpdyv8oO3j.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:	49
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@53/24@7/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.1% (good quality ratio 7.9%) • Quality average: 60.6% • Quality standard deviation: 33%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:13:59	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\explorer.lnk
10:14:15	API Interceptor	56x Sleep call for process: Windows Update.exe modified
10:14:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 61bc7bd88d10e97264127fe545415b17 " C:\Users\user\AppData\Roaming\RedLine.exe" ..
10:14:25	API Interceptor	2x Sleep call for process: dw20.exe modified
10:14:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming \WindowsUpdate.exe
10:14:37	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 61bc7bd88d10e97264127fe545415b17 "C:\Users\user\AppData\Roaming\RedLine.exe" ..
10:14:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
10:14:53	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run 61bc7bd88d10e97264127fe545415b17 "C:\Users\user\AppData\Roaming\RedLine.exe" ..
10:15:01	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\61bc7bd88d10e97264127fe545415b17.exe
10:15:30	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_windows update.e_88669d6d392fdabab3f150c24b7e9ac915a06366_00000000_10d37750\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.402933249166855
Encrypted:	false
SSDEEP:	192:7Z82iVXa6nzCr69+k/NRWsX1OzviHk0KHvI7Dp7/u7s7S274It:l82+aMVbovhOt7/u7s7X4It
MD5:	5CE90DFC6068FC01BFAF7F151CF34B16
SHA1:	886CA7A3E79ECF401FAED7EF174A6591C06AE700
SHA-256:	70A3B65501A1CC41F26C156B4154A0D735D4ED9A6225AA1FDF5EE688D667442C
SHA-512:	CFBF12F5A9D85813D2F21F370488A5B43BF9B96ADC2200E8F59D7CCD24AB62D887B4DE1A63704798DE80CAE01E7170D3A9D19080E7F2A42DD609EEC5D27AC96
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.1.7.3.2.8.6.0.3.5.7.3.9.9.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.1.7.3.2.8.6.3.9.0.4.2.6.7.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.4.3.5.0.a.d.e.-.b.6.9.5.-.4.d.e.2.-.8.8.7.7.-.7.2.1.1.f.c.e.2.e.5.d.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.h.u.l.l.i...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.f.8.-.0.0.0.1.-.0.0.1.c.-.e.b.e.d.-.1.4.1.1.a.8.d.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.6.c.c.9.4.0.d.7.a.0.d.3.0.a.e.2.8.3.f.a.7.7.b.e.8.f.e.6.4.d.3.0.0.0.0.0.0.0.0.!.0.0.0.0.6.e.e.f.0.5.8.8.d.d.0.3.8.f.5.f.f.2.a.7.3.c.7.0.a.d.d.3.6.c.1.6.5.9.4.9.5.3.2.2.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.0././.2.9.:.1.7.:.5.3.:.3.7.!.0.!.W.i.n.d.o.w.s. .U.p.d.a.t.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6493.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5676
Entropy (8bit):	3.7219070243581234
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3iSS63ia6eYZ5BSfgRAgVBCaM18L1fao0m:Rrl7r3GLNiSS63ia6eYZ5BSgCp18L1fZ
MD5:	B42975E415A75C4CC8FA14FE1DC97DD1
SHA1:	A7584F6F58ECEA3D9F5BA379C927C1C4B8B5FB3F
SHA-256:	2F88C278B6B57892FEDEF357323FAD2D980AA128CFEF95A5E43B1386A5E687F0
SHA-512:	40216909F03821637F7121DA2199E2353D264E95656E0D4150887F8E6A8FB11886F34EF447008BAEA567D5CA8D9D71CD907A5853D91D9A072C59DDFB4CCC3F37
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.6.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6688.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4699
Entropy (8bit):	4.455476964891945
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9jzWSC8BN8fm8M4JFKsKWuFdP+q8vRKWqb/uEB+/hKd:uITf9oCSN0JFKXPKAWEk/hKd
MD5:	8CA2F90D6BABEB2530A1B91B2B9FF6A6
SHA1:	0CD4F5CF2300A9B07862DC4ED5C11E41D5BAF876
SHA-256:	7D828E529450D49F9B40BECE93A43007EEC440C228E77366A2CA9EB72FB7B377
SHA-512:	E90C156862267DC16351CF113A413C03DFB78CFD17B532C352A5E3A588D1B4CA09D45C5EA364F200D163F00C643D85F332225CAAE418824EF90C12D8169C585
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6688.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1260204" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\RedLine.MainPanel-cracked.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.278948378331044
Encrypted:	false
SSDEEP:	12:Q3LaJcP0/9UkB9t0kaHYGLi1B01kKVdisk7v:ML2pBLaYgioQF
MD5:	CB9A918AA4F64DF8162B857C63195287
SHA1:	70E078D64F44CCB2BD89B106204E14D9E3B58894
SHA-256:	104503FEB03BB8F7D338CDB64A0B2E2B608A966BDFE899142C9762B2D21F9260
SHA-512:	3C1EB042EA3D9892271ADD759E516FE626209D2F5F5EC25A309380F16935FE8640B4751529CD6B5826D387DED9F7F2069F54095BCA7F3A19AE2116B81C30595B
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.VisualBas#\76002c3c0a2b9f0c8687ad35e8d9d309\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\454c09ea87bde1d5f545d60232083b79\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Keylogger.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Keylogger.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\HOST.bat	
Process:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	4.602721733839044
Encrypted:	false
SSDEEP:	6:h4xBuAR04xBuAR04xBuAR04xBuARm8HP04xBuARm8Hrq9i5HP04xBuARm8Hrq9i4:WxBhxBhxBhxBLxBygxBy9
MD5:	ACE9684D1899236D68944B8FD65D1FB5
SHA1:	558A8B99483E4F0D8D2D0C6A509589901265881B
SHA-256:	52DE0F6975F003E8F79F37F30BE69CB38F3679E23DAC8F0446625A76C14A8B19
SHA-512:	937F39AD2910D62BDA8FD71D46083517D380D07C610794461FB62D3A9A66C602D36ECE1B5AEE24649EE521AF6768C7C89827E8065692CC6CB0A12FBFCA9127D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\HOST.bat	
Preview:	@echo off..cd %systemroot%\system32\drivers\etc..exit..@echo off..cd %systemroot%\system32\drivers\etc..exit..@echo off..cd %systemroot%\system32\drivers\etc..exit..@echo off..cd %systemroot%\system32\drivers\etc..echo 127.0.0.1 virustotal.com >> hosts..exit..@echo off..cd %systemroot%\system32\drivers\etc..echo 127.0.0.1 virustotal.com >> hosts..echo 127.0.0.1 yandex.com >> hosts..exit..@echo off..cd %systemroot%\system32\drivers\etc..echo 127.0.0.1 virustotal.com >> hosts..echo 127.0.0.1 yandex.com >> hosts..exit..

C:\Users\user\AppData\Local\Temp\Keylogger.exe	
Process:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.503682543410338
Encrypted:	false
SSDEEP:	6144:huxqV1dNbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9Y:RdNQtqB5urTIoYWBQk1E+VF9mOx9oiL
MD5:	C4E4A84909D8FF8DD222B8252365985D
SHA1:	6EEF0588DD038F5FF2A73C70ADD36C1659495322
SHA-256:	14ADE1921A7BFE68DBFD21BFEB14BBEF6B89ED0DD15E9FBFA79A985EB42959F2
SHA-512:	24CB338CAE623B7532AC04EE25CC41A8B319D6F80324F3A411796633969604925A857353655BE39D7E2254465F6830E4D6F0A04265C34AB042939EB6AD5D3672
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!5|a.....4..... .....@.. ....@.....K.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.reloc.....` .....".....@..B.....H.....0}.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....~.....~....o....o.....1.~....~....o.....o.....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(.....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe	
Process:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	4.7460869785957795
Encrypted:	false
SSDEEP:	1536:la5jbMQXU4hH8yvmYRVFykX84Jw08W6ArYVTsr7KRbLfC:o5jJXUQCk/raXbO
MD5:	098F7F40BACA320377ECA83FBF87F534
SHA1:	1C14C269465D850550EB7DC955E5CA5A0FA2CEC2
SHA-256:	42B18977DAC9E72BBC4B9FA1A61085CD8A96CD99E59421196AA8AA0D8D4CF225
SHA-512:	B6270744603D1D842E42827E561C85A130DAB6859FEFAC2F255B8911175D2394E0D8A48B5F676EC7C4CF4342CD088CB3A99C7379F17171CF5944A07E11D5D577
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Kxa.....~.... .....@.. ....@.....,...O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....`.....H.....6..0.....L....5..p.....&.(.....*..*..(.....*..s.....s.....s.....s.....s.....*....0.....~....o....+..* .0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....{....(...+}....{....+..*.0..7.....{.....,..+%.....,r...ps....z...|....o...+..*..0..... .....,.....o....-..+.....9....~.....,3~.....(...

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Process:	C:\Users\user\AppData\Local\Temp\Keylogger.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.387380345401073
Encrypted:	false
SSDEEP:	3:oNWXp5cViEaKC59KuCa:oNWXp+NaZ5v
MD5:	95FC50C7E40BB0D5EBD49FCBEE4E890D

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
SHA1:	E5086A9390CC8D6F512A206AB1AC4309A4CC4326
SHA-256:	DC88107DF527833D0D8B7AC45D31AF0E5343AE36AB9725016B046CDD77E46EC7
SHA-512:	4AC9E01163C00CC874BDBE1E4B5BF2463F8B53B9102705C774C790D8DFD8AEAD662DEDA812CF457022820FFD8174A1CD0275601C4BC6E4CCDB7E5A80CD52F99
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe

C:\Users\user\AppData\Local\Temp\ViRuS.exe	
Process:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	46132
Entropy (8bit):	5.26909765114528
Encrypted:	false
SSDEEP:	768:dmiiqTfk2AMRGwlFgOrjsI5Z52ulLGM88VI02foeZSgTi10U:dpTfDbGwlF9nsI5Z52ulLGM88VI02foT
MD5:	D0F09063EA6922ACBFC734145FA48203
SHA1:	48253D06D8D053A4433B679E56270553D4F7FD66
SHA-256:	71B96AF827245221A3D2AA884636F20BF41627DFC079A02D5DE58CD58C9A0111
SHA-512:	E1DAC2DD5A8F05ED26C817CADEDD3A8B0124A15D257BDAB434E88BE2300E64BA8270A0DCFA5990CA8A81D36E274CC77BE843A31E6CC10A074B7DFE4B24C71A3F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 83%, Browse • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....si..si..si..ld..si.Rich.si.....PE..L...j..G.....`... ..<.....p....@.....~.....l..(.....(... .....text....]......`..... ..`.data... .....p.....@....rsrc.....p.....@..@..:@.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\bhvB786.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x91cb4e71, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:C28A2Ta0xucRfDw/9iD0Xko5QqbMgSFDb7uBis:cRfDc/y
MD5:	228AC2AB635442EBC4A1C3F2C2ACBB8C
SHA1:	75651BEDDE6473D1F40F4F287EB13A858862AF2C
SHA-256:	9E3D696D433E10116BD7BC81039C13A4A496F5D38429745A5891EF46BDCFDC4F
SHA-512:	0A75529DEEF98D48415699EEE1FD76BDE00879AF99E13D78F6EB62F4EAE62B63D0FC54A48E1D98EA3CB567FB461BEF601AC3AF86263FABB0487181F40FB8B15A
Malicious:	false
Reputation:	unknown
Preview:	..Nq... .....F1.....te3....wg.....o.....6....y.....y..h.q.....6..43....wl.....Z.....B..... .....y..... .....{!}r....y.s.....3G?....y..... .....

C:\Users\user\AppData\Local\Temp\hhzclipper.exe	
Process:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.0620477915188244
Encrypted:	false
SSDEEP:	96:efGLLgKK3A/A/Aa5X5X5YggFjju++7J0sLQP6/4RCBvPgKrzwWCLxQ:GGLLgKK3eeB5X5X5YggFjju++JQP6/4Q
MD5:	FC07BE5E90A1FFA22B22D3BC58A43E58
SHA1:	07BCA65E7754F4EA6093036D83549734AAB53758
SHA-256:	7DE848E40DA073492C4F20587C4F53EC43CDFB3C199C6B76F58218D1E696DB1C
SHA-512:	6E8C6A203A943D39DFE506F177AD9282C6645EB61306AC345A4AC21899F9833B22792DC23B8C24F439198C99DCC5D5F6301FBA1D8BB65EA32C812DD159F8927
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\hhzclipper.exe	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{a...../... ...@....@.. ....@.....\/..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B...../.....H.....(..p.....0.....r...p.r...p.r...p.r...p.r...p..r...p..r...p..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\61bc7bd88d10e97264127fe545415b17.exe	
Process:	C:\Users\user\AppData\Roaming\RedLine.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	4.7460869785957795
Encrypted:	false
SSDEEP:	1536:la5jbMQXU4hH8yvmYRVFykX84Jw08W6ArYVTsr7KRbLfC:o5jJXUQCk/raXbO
MD5:	098F7F40BACA320377ECA83FBF87F534
SHA1:	1C14C269465D850550EB7DC955E5CA5A0FA2CEC2
SHA-256:	42B18977DAC9E72BBC4B9FA1A61085CD8A96CD99E59421196AA8AA0D8D4CF225
SHA-512:	B6270744603D1D842E42827E561C85A130DAB6859FEFAC2F255B8911175D2394E0D8A48B5F676EC7C4CF4342CD088CB3A99C7379F17171CF5944A07E11D5D577
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Kxa.....~.... .....@.. ....@.....,...O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....`.....H.....6..0.....L....5..p.....&.(.....*..*..(.....*..s.....s.....s.....s.....s.....*....0.....~....o.....+..* .0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....{....(...+}.....{.....+..*.0..7.....{.....,..+%.....,r...ps....z...|....o...+..*..0..... .....,.....o....-..+.....9....~.....,3~.....(...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\explorer.lnk	
Process:	C:\Users\user\AppData\Local\Temp\ViRuS.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Icon number=0, Archive, ctime=Thu Nov 18 17:13:53 2021, mtime=Thu Nov 18 17:13:53 2021, atime=Thu Nov 18 17:13:52 2021, length=46132, window=hide
Category:	dropped
Size (bytes):	1791
Entropy (8bit):	3.125340834929565
Encrypted:	false
SSDEEP:	24:8dlQxhubkkiAKmG+/7X+IMs416EbmX7aB6m:8nZJBDdXfMT1XbmmB6
MD5:	F50DBACEDA242CDA5A8F9AA8FE302153
SHA1:	D3301CC2B8BBEC48B549220214B557160C5953EA
SHA-256:	E5CC4DA8E6EFAAC1CD3EF645A05FCF844D007CCDB14CF514AD8A1978BE16BDC1
SHA-512:	7966356678C722451ED823C576E789AD061390161EA3DCC180A16262BC620E0C1A10B2937844C1FF34E7B4CDF66F82251945C099201EBDA21DAFB525A6A3CC78
Malicious:	false
Reputation:	unknown
Preview:	L.....F.@.. ....gP.....K,U.....0.....4.....G....P.O. .:i.....+00.../C:\.....V.1.....7S{y..Windows.@.....L..rS.....c.k.W.i.n.d.o.w.s.....Z.1. ....7Spy..System32..B.....L..rS.....I..S.y.s.t.e.m.3.2.....h.2.4...rS.. .USER32~1.EXE..L.....rS..rS.....>}.....u.s.e.r.3.2.d.l.l...e.x.e.....P.....-.... ...O.....m.{.....C:\Windows\System32\user32dll.exe..9....\....\....\....\....\....\....\....\....\....\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.u.s.e.r.3.2.d.l.l...e.x.e...C.:.\.W.i.n.d.o.w.s.\.e. x.p.l.o.r.e.r...e.x.e.....%SystemRoot%\explorer.exe..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.e.x.p.l.o.r.e.r...e.x.e.....

C:\Users\user\AppData\Roaming\RedLine.exe	
Process:	C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	4.7460869785957795
Encrypted:	false
SSDEEP:	1536:la5jbMQXU4hH8yvmYRVFykX84Jw08W6ArYVTsr7KRbLfC:o5jJXUQCk/raXbO
MD5:	098F7F40BACA320377ECA83FBF87F534
SHA1:	1C14C269465D850550EB7DC955E5CA5A0FA2CEC2
SHA-256:	42B18977DAC9E72BBC4B9FA1A61085CD8A96CD99E59421196AA8AA0D8D4CF225
SHA-512:	B6270744603D1D842E42827E561C85A130DAB6859FEFAC2F255B8911175D2394E0D8A48B5F676EC7C4CF4342CD088CB3A99C7379F17171CF5944A07E11D5D577
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Kxa.....~.... .....@.. ....@.....,...O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....`.....H.....6..0.....L....5..p.....&.(.....*..*..(.....*..s.....s.....s.....s.....s.....*....0.....~....o.....+..* .0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....{....(...+}.....{.....+..*.0..7.....{.....,..+%.....,r...ps....z...|....o...+..*..0..... .....,.....o....-..+.....9....~.....,3~.....(...

C:\Users\user\AppData\Roaming\Windows Update.exe	
Process:	C:\Users\user\AppData\Local\Temp\Keylogger.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.503682543410338
Encrypted:	false
SSDEEP:	6144:huxqV1dNbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9Y:RdNQtqB5urTIoYWBQk1E+VF9mOx9oiL
MD5:	C4E4A84909D8FF8DD222B8252365985D
SHA1:	6EEF0588DD038F5FF2A73C70ADD36C1659495322
SHA-256:	14ADE1921A7BFE68DBFD21BFEB14BBEF6B89ED0DD15E9FBFA79A985EB42959F2
SHA-512:	24CB338CAE623B7532AC04EE25CC41A8B319D6F80324F3A41179663396960492 5A857353655BE39D7E2254465F6830E4D6F0A04265C34AB042939EB6AD5D3672
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!5|a.....4..... .....@.. ....@.....K.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.reloc.....` .....".....@..B.....H.....0}.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....~.....~.....o....o.....1.~.....~....o.....o....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	533504
Entropy (8bit):	6.503682543410338
Encrypted:	false
SSDEEP:	6144:huxqV1dNbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9Y:RdNQtqB5urTIoYWBQk1E+VF9mOx9oiL
MD5:	C4E4A84909D8FF8DD222B8252365985D
SHA1:	6EEF0588DD038F5FF2A73C70ADD36C1659495322
SHA-256:	14ADE1921A7BFE68DBFD21BFEB14BBEF6B89ED0DD15E9FBFA79A985EB42959F2
SHA-512:	24CB338CAE623B7532AC04EE25CC41A8B319D6F80324F3A41179663396960492 5A857353655BE39D7E2254465F6830E4D6F0A04265C34AB042939EB6AD5D3672
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!5|a.....4..... .....@.. ....@.....K.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.reloc.....` .....".....@..B.....H.....0}.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....~.....~.....o....o.....1.~.....~....o.....o....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0

C:\Users\user\AppData\Roaming\pid.txt	
Encrypted:	false
SSDEEP:	3:C7:C7
MD5:	81BC798A42A7CE40810BF523F24DEEE1
SHA1:	2EB42F6F5AA9B4FEE8A34200D60567A93CBC72CE
SHA-256:	1CC4C660D80F3452841386109DEEAFFE554F4FD47A5409F614BD6C1B53C78C65
SHA-512:	ED786180AC7491F2C13A7E6453FD329FC53659F4F454BFB704B12DA7617BB94461D78C12FF7A1CDD0255815EA189684344EFABD86304146C98A9650257C89B9C
Malicious:	false
Reputation:	unknown
Preview:	5248

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.441568140944513
Encrypted:	false
SSDEEP:	3:oNWXp5cViEaKC59KYr4a:oNWXp+NaZ534a
MD5:	6078085422A31D60FCEB24D4FA24B6E8
SHA1:	0CD056478F3D877B3D44C7B439485B1ACFD78F5A
SHA-256:	9113E6728CEB1F460E3CEAB19852A31602CD77A92E7B861802FE339FD5CFD837
SHA-512:	22CE5D96BB25519CB14F27BDB44D7FAEDC6D5C8B8F81A1F972EA638BF9731D8793C98359D7C9476D50AF46346E0964E82F5B0B2F8B1B6763B078D2B045FB2EA 1
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Roaming\Windows Update.exe

C:\Windows\SysWOW64\user32dll.exe	
Process:	C:\Users\user\AppData\Local\Temp\ViRuS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	46132
Entropy (8bit):	5.26909765114528
Encrypted:	false
SSDEEP:	768:dmiiqTfk2AMRGwlFgOrjsI5Z52ulLGM88VI02foeZSgTi10U:dpTfDbGwlF9nsI5Z52ulLGM88VI02foT
MD5:	D0F09063EA6922ACBFC734145FA48203
SHA1:	48253D06D8D053A4433B679E56270553D4F7FD66
SHA-256:	71B96AF827245221A3D2AA884636F20BF41627DFC079A02D5DE58CD58C9A0111
SHA-512:	E1DAC2DD5A8F05ED26C817CADEDD3A8B0124A15D257BDAB434E88BE2300E64BA8270A0DCFA5990CA8A81D36E274CC77BE843A31E6CC10A074B7DFE4B24C7 1A3F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 83%, Browse • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....si..si..si..ld..si.Rich.si.....PE..L...j..G.....`... .. ....<.....p....@.....~.....l..(.....(... .....text....]....`..... ..`.data... .....p.....@....rsrc.....p.....@..@..:@.....MSVBVM60.DLL..... ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2756168590544
Encrypted:	false
SSDEEP:	12288:hfnlScmddpKhnku1M5h0NXtX3ZQL1xQHwrzzmMB+aUn+frp0BrBN1:5nlScmddpKhnkuxH
MD5:	6F6341035C32C699CCB490E03BA51DA2
SHA1:	AB3534EB33DD4685111AFDEB644B8ACA5098DDA8
SHA-256:	D44A0D22E8F8E5723BE787028A956EEFCC7BCCC5960B60FB9606097C2B1BEBDD
SHA-512:	928BE07358B6277D052DCF2FFA8C1571A1F2DA2AE55A09FCA231F768B57811B6BBB1AB3204D3D447341D778AE8428C9E4948499404B52606A2C5DD11D4F0B50
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve	
Reputation:	unknown
Preview:	regfZ...Z...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.g&..... ...."G..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	4.204425478661901
Encrypted:	false
SSDEEP:	768:+h8dCkpMwqharRCXw5ftx1zJ4XVFFZ7FBqXceq5QMVyi6aC4LX+uzuRDTm:EfaBfy2CRRT4
MD5:	CE8E365BA34D14C0A14087AEB24CFCC4
SHA1:	58EE19555F73CCE80A027EC17DA6D9A4D16586E6
SHA-256:	5AC5EC00FEF748A4078CBFD61991BBA6A688FA8E349BB8DB1731147E997B4C11
SHA-512:	9CF04D31A6D46ED9D84A9FE4BC5C6D3D6EC793D653B96964DD56173FDD59EC44CDA3254500DC9F5A1557C821BBE7C34030C05F98D6DDAE2FB63F150004D8C 79
Malicious:	false
Reputation:	unknown
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.g&..... ...."GHvLE.....Y.....vT.....L&u.GY..... ....P.....0..... ..hbin.....p.\..,.....nk,..g&..... .....&...{ad7 9c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..g&..... ....Z.....Root.....lf.....Root....nk ..g&.....}..... .....*..... DeviceCensus.....vk.....

\Device\ConDrv	
Process:	C:\Windows\System32\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	313
Entropy (8bit):	4.971939296804078
Encrypted:	false
SSDEEP:	6:/ojfKsUTGN8Ypox42k9L+DbGMKeQE+vigqAZs2E+AYeDPO+Yswyha:wjPIGNrkHk9iaeIM6ADDPOHyha
MD5:	689E2126A85BF55121488295EE068FA1
SHA1:	09BAAA253A49D80C18326DFBCA106551EBF22DD6
SHA-256:	D968A966EF474068E41256321F77807A042F1965744633D37A203A705662EC25
SHA-512:	C3736A8FC7E6573FA1B26FE6A901C05EE85C55A4A276F8F569D9EADC9A58BEC507D1BB90DBF9EA62AE79A6783178C69304187D6B90441D82E46F5F56172B5C5 C
Malicious:	false
Reputation:	unknown
Preview:	..IMPORTANT: Command executed successfully...However, "netsh firewall" is deprecated;..use "netsh advfirewall firewall" instead...For more information on using "netsh advfirewall firewall" commands..instead of "netsh firewall", see KB article 947709..at https://go.microsoft.com/fwlink/?linkid=121488 .....Ok.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.7405121102619034
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	Hpdyv8oO3j.exe
File size:	1634464
MD5:	dffaf08a25150b38c19210c180862aeb
SHA1:	a28b135b64a08d5ed30621aac5c3e955d4d090fb
SHA256:	8fdbfbf55033187c6a4d3cd7d42394cd56cbd3b5a9dc905e72aef2886172be36

General

SHA512:	140b3431fb93d4af25df7da68b9dea8eec93e721f40831c12a0a2acb0e9fd1bda23a9d9665b5d18a39a2424bf5b57a2118dab705bfaabd0ce759e3fe0786abe7
SSDEEP:	24576:Db9maw2TucZ2p7oPGutOb82k3QfRq661wRISp5iygGVBi9NTFABQHFidcQKwY:VgZWfu79UOq61IYLOZUQHifKwY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Q.....X..... ....@.....`..... .....

File Icon



Icon Hash:	70f0b2e8c8cce071

Static PE Info

General

Entrypoint:	0x401ae1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x51BC99EC [Sat Jun 15 16:44:28 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d5d9d937853db8b666bd4b525813d7bd

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc26	0xe00	False	0.479352678571	data	5.14633256781	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x4c0	0x600	False	0.405598958333	data	4.21235747943	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0xd6f0	0x600	False	0.169270833333	data	1.7255508052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x174bf0	0x174c00	False	0.979429310236	data	7.95139965452	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/18/21-10:14:13.549647	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	104.16.155.36	192.168.2.3
11/18/21-10:15:00.459104	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49792	104.16.154.36	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2021 10:14:12.731645107 CET	192.168.2.3	8.8.8.8	0x421f	Standard query (0)	231.58.0.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2021 10:14:13.398452044 CET	192.168.2.3	8.8.8.8	0xb8e2	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2021 10:14:15.762671947 CET	192.168.2.3	8.8.8.8	0xb79a	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:00.053471088 CET	192.168.2.3	8.8.8.8	0xa891	Standard query (0)	231.58.0.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 18, 2021 10:15:00.304965019 CET	192.168.2.3	8.8.8.8	0x26bc	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:02.745244980 CET	192.168.2.3	8.8.8.8	0x1d23	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:16.821176052 CET	192.168.2.3	8.8.8.8	0xbc52	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2021 10:14:12.751557112 CET	8.8.8.8	192.168.2.3	0x421f	Name error (3)	231.58.0.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2021 10:14:13.421236038 CET	8.8.8.8	192.168.2.3	0xb8e2	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2021 10:14:13.421236038 CET	8.8.8.8	192.168.2.3	0xb8e2	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2021 10:14:15.791515112 CET	8.8.8.8	192.168.2.3	0xb79a	No error (0)	smtp.gmail.com		173.194.79.109	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:00.073345900 CET	8.8.8.8	192.168.2.3	0xa891	Name error (3)	231.58.0.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 18, 2021 10:15:00.328694105 CET	8.8.8.8	192.168.2.3	0x26bc	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:00.328694105 CET	8.8.8.8	192.168.2.3	0x26bc	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:02.771996975 CET	8.8.8.8	192.168.2.3	0x1d23	No error (0)	smtp.gmail.com		173.194.79.108	A (IP address)	IN (0x0001)
Nov 18, 2021 10:15:16.849581003 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	smtp.gmail.com		173.194.79.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

Copyright Joe Security LLC 2021

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49752	104.16.155.36	80	C:\Users\user\AppData\Roaming\Windows Update.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:14:13.524677992 CET	748	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2021 10:14:13.549647093 CET	749	IN	HTTP/1.1 403 Forbidden Date: Thu, 18 Nov 2021 09:14:13 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Referrer-Policy: same-origin Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cf_bm=sGeod6pqVWjcwREELm2hUH2GgAdW_2GQyVQFKmuAcw0-1637226853-0-ARb8/mXyrtsjl iF6MoAc1RTKm13uI/eP7YlvFz7ZWBMjq2DYNWHf6wU8P4W3in6z8BV4TXLAYgb9S5ghyt8nUT4=; path=/; expires=Thu, 18-Nov-21 09:44:13 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6b00165a9d85690a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49792	104.16.154.36	80	

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:15:00.430659056 CET	1636	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 18, 2021 10:15:00.459104061 CET	1637	IN	HTTP/1.1 403 Forbidden Date: Thu, 18 Nov 2021 09:15:00 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Referrer-Policy: same-origin Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cf_bm=_VxCpL1SUogQPkmhm6XJQzy_263PsYORKxhnP5Lzpu8-1637226900-0-AakJJ2rong7ag BiGXb/Yc2BMeTYb8+YfO1kR1pbeDWQZeZMuafai1azbDQQgGLp6uCRe9S4dAlA9ilezE9rCYhl=; path=/; expires=Thu, 18-Nov-21 09:45:00 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6b00177fbd724e44-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 18, 2021 10:14:16.057013035 CET	587	49753	173.194.79.109	192.168.2.3	220 smtp.gmail.com ESMTP v3sm1390611edc.69 - gsmtp
Nov 18, 2021 10:14:16.073266983 CET	49753	587	192.168.2.3	173.194.79.109	EHLO 035347
Nov 18, 2021 10:14:16.104752064 CET	587	49753	173.194.79.109	192.168.2.3	250-smtp.gmail.com at your service, [84.17.52.63] 250-SIZE 35882577 250-8BITMIME 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250 SMTPUTF8
Nov 18, 2021 10:14:16.153516054 CET	49753	587	192.168.2.3	173.194.79.109	STARTTLS
Nov 18, 2021 10:14:16.181858063 CET	587	49753	173.194.79.109	192.168.2.3	220 2.0.0 Ready to start TLS
Nov 18, 2021 10:15:02.877749920 CET	587	49805	173.194.79.108	192.168.2.3	220 smtp.gmail.com ESMTP dm5sm751309ejc.81 - gsmtp
Nov 18, 2021 10:15:02.878535032 CET	49805	587	192.168.2.3	173.194.79.108	EHLO 035347
Nov 18, 2021 10:15:03.112066984 CET	587	49805	173.194.79.108	192.168.2.3	220 smtp.gmail.com ESMTP dm5sm751309ejc.81 - gsmtp
Nov 18, 2021 10:15:03.268135071 CET	49805	587	192.168.2.3	173.194.79.108	EHLO 035347

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 18, 2021 10:15:03.298783064 CET	587	49805	173.194.79.108	192.168.2.3	250-smtp.gmail.com at your service, [84.17.52.63] 250-SIZE 35882577 250-8BITMIME 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250 SMTPUTF8
Nov 18, 2021 10:15:03.543004036 CET	49805	587	192.168.2.3	173.194.79.108	STARTTLS
Nov 18, 2021 10:15:03.572115898 CET	587	49805	173.194.79.108	192.168.2.3	220 2.0.0 Ready to start TLS
Nov 18, 2021 10:15:16.926930904 CET	587	49808	173.194.79.108	192.168.2.3	220 smtp.gmail.com ESMTP r25sm642291edt.21 - gsmtp

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Hpdyv8oO3j.exe PID: 6436 Parent PID: 6108

General

Start time:	10:13:43
Start date:	18/11/2021
Path:	C:\Users\user\Desktop\Hpdyv8oO3j.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Hpdyv8oO3j.exe"
Imagebase:	0x400000
File size:	1634464 bytes
MD5 hash:	DFFAF08A25150B38C19210C180862AEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: Keylogger.exe PID: 4492 Parent PID: 6436

General

Start time:	10:13:49
Start date:	18/11/2021

Path:	C:\Users\user\AppData\Local\Temp\Keylogger.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Keylogger.exe"
Imagebase:	0x760000
File size:	533504 bytes
MD5 hash:	C4E4A84909D8FF8DD222B8252365985D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.345938091.0000000000762000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.345938091.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.345938091.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.345938091.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.345938091.0000000000762000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000000.314643771.0000000000762000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000000.314643771.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000000.314643771.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000000.314643771.0000000000762000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000000.314643771.0000000000762000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000003.339296284.0000000000E97000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000003.339296284.0000000000E97000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000003.339296284.0000000000E97000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000003.339296284.0000000000E97000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000003.339296284.0000000000E97000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\Keylogger.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: hhzclipper.exe PID: 1244 Parent PID: 6436

General

Start time:	10:13:50
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Local\Temp\hhzclipper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\hhzclipper.exe"
Imagebase:	0x1e0000
File size:	6144 bytes
MD5 hash:	FC07BE5E90A1FFA22B22D3BC58A43E58
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: RedLine.MainPanel-cracked.exe PID: 4140 Parent PID: 6436

General

Start time:	10:13:50
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe"
Imagebase:	0x550000
File size:	77824 bytes
MD5 hash:	098F7F40BACA320377ECA83FBF87F534
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: 00000004.00000002.344112668.0000000002630000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.344112668.0000000002630000.00000004.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.344112668.0000000002630000.00000004.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000004.00000002.344112668.0000000002630000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.344202284.0000000002AC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.344202284.0000000002AC1000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000004.00000002.344202284.0000000002AC1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 89%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: RedLine.MainPanel-cracked.exe PID: 7032 Parent PID: 6436

General

Start time:	10:13:51
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\RedLine.MainPanel-cracked.exe"
Imagebase:	0x340000
File size:	77824 bytes
MD5 hash:	098F7F40BACA320377ECA83FBF87F534
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000005.00000002.339955429.0000000002861000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000005.00000002.339955429.0000000002861000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000005.00000002.339955429.0000000002861000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: 00000005.00000002.339619983.00000000024B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000005.00000002.339619983.00000000024B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000005.00000002.339619983.00000000024B0000.00000004.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000005.00000002.339619983.00000000024B0000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 3348 Parent PID: 6436

General

Start time:	10:13:52
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\HOST.bat" "
Imagebase:	0xd80000
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 Read

Analysis Process: conhost.exe PID: 6232 Parent PID: 3348

General

Start time:	10:13:52
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: ViRuS.exe PID: 2988 Parent PID: 6436

General

Start time:	10:13:52
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Local\Temp\ViRuS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\ViRuS.exe"
Imagebase:	0x400000
File size:	46132 bytes
MD5 hash:	D0F09063EA6922ACBFC734145FA48203
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 83%, Metadefender, Browse • Detection: 93%, ReversingLabs
Reputation:	low

Copyright Joe Security LLC 2021

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: attrib.exe PID: 5332 Parent PID: 2988

General

Start time:	10:13:54
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\attrib.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\attrib.exe" +r +h +s +a "C:\Windows\system32\user32dll.exe
Imagebase:	0xf90000
File size:	19456 bytes
MD5 hash:	A5540E9F87D4CB083BDF8269DEC1CFF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: 5308 Parent PID: 5332

General

Start time:	10:13:54
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: attrib.exe PID: 7160 Parent PID: 2988

General

Start time:	10:13:55
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\attrib.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\attrib.exe" +r +h +s +a "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\explorer.lnk
Imagebase:	0xf90000

Copyright Joe Security LLC 2021

File size:	19456 bytes
MD5 hash:	A5540E9F87D4CB083BDF8269DEC1CFF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: 7140 Parent PID: 7160

General

Start time:	10:13:55
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 7116 Parent PID: 2988

General

Start time:	10:13:55
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im "ViRuS.exe"
Imagebase:	0xee0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 7120 Parent PID: 7116

General

Start time:	10:13:56
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: RedLine.exe PID: 4236 Parent PID: 4140

General

Start time:	10:14:02
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Roaming\RedLine.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\RedLine.exe"
Imagebase:	0x580000
File size:	77824 bytes
MD5 hash:	098F7F40BACA320377ECA83FBF87F534
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000010.00000002.569953826.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000010.00000002.569953826.0000000002A81000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000010.00000002.569953826.0000000002A81000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: 00000010.00000002.569803952.0000000002700000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000010.00000002.569803952.0000000002700000.00000004.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000010.00000002.569803952.0000000002700000.00000004.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000010.00000002.569803952.0000000002700000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 89%, ReversingLabs

Analysis Process: Windows Update.exe PID: 5624 Parent PID: 4492

General

Start time:	10:14:03
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windows Update.exe"
Imagebase:	0xd40000
File size:	533504 bytes
MD5 hash:	C4E4A84909D8FF8DD222B8252365985D
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: 00000011.00000002.401046205.000000000384C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.401022146.0000000003844000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000002.401022146.0000000003844000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000002.398362779.00000000033D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.398362779.00000000033D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source:

00000011.00000002.398362779.00000000033D1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000011.00000002.404757917.0000000007F20000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000000.344079662.0000000000D42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000000.344079662.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000000.344079662.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.344079662.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000000.344079662.0000000000D42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000000.345013885.0000000000D42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000000.345013885.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000000.345013885.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.345013885.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000000.345013885.0000000000D42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000002.395985311.0000000000D42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000002.395985311.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000002.395985311.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000002.395985311.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000002.395985311.0000000000D42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000011.00000002.404673570.0000000007D50000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000000.344577031.0000000000D42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000000.344577031.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000000.344577031.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.344577031.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000000.344577031.0000000000D42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000003.370310625.0000000006DFE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000003.370310625.0000000006DFE000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000003.370310625.0000000006DFE000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000003.370310625.0000000006DFE000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000003.370310625.0000000006DFE000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000002.401457902.00000000043D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000002.402244108.0000000004591000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000011.00000000.343560898.0000000000D42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000011.00000000.343560898.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000011.00000000.343560898.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.343560898.0000000000D42000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000011.00000000.343560898.0000000000D42000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Windows Update.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: user32dll.exe PID: 7128 Parent PID: 3352

General

Start time:	10:14:08
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\user32dll.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\user32dll.exe"
Imagebase:	0x400000
File size:	46132 bytes
MD5 hash:	D0F09063EA6922ACBFC734145FA48203
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 83%, Metadefender, Browse • Detection: 93%, ReversingLabs

Analysis Process: taskkill.exe PID: 7156 Parent PID: 7128

General

Start time:	10:14:09
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im "user32dll.exe"

Imagebase:	0xee0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7080 Parent PID: 7156

General

Start time:	10:14:09
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 7096 Parent PID: 4236

General

Start time:	10:14:14
Start date:	18/11/2021
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\RedLine.exe" "RedLine.exe" ENABLE
Imagebase:	0x7ff603860000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6480 Parent PID: 7096

General

Start time:	10:14:15
Start date:	18/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Analysis Process: dw20.exe PID: 4332 Parent PID: 5624

General

Start time:	10:14:16
Start date:	18/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2528
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vbc.exe PID: 6444 Parent PID: 5624

General

Start time:	10:14:21
Start date:	18/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt"
Imagebase:	
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_MailPassView, Description: Yara detected MailPassView, Source: 00000019.00000002.567099655.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: vbc.exe PID: 1364 Parent PID: 5624

General

Start time:	10:14:21
Start date:	18/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt"
Imagebase:	
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vbc.exe PID: 1980 Parent PID: 5624

General

Start time:	10:14:23
Start date:	18/11/2021

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\holderwb.txt" /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt"
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.00000000.394707935.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000000.395296595.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.412155949.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000000.393916948.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021