ID: 547727
Sample Name:
SW0P9o9ksjpBsnr.exe
Cookbook: default.jbs
Time: 15:04:39
Date: 04/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SW0P9o9ksjpBsnr.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 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 6
AV Detection: 6
Exploits: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
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 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 47
General 47
File Icon 48
Static PE Info 48
General 48
Entrypoint Preview 48
Data Directories 48
Sections 48
Resources 48
Imports 48
Version Infos 48
Network Behavior 48
Snort IDS Alerts 49
Network Port Distribution 49
TCP Packets 49
UDP Packets 49
DNS Queries 49

DNS Answers 49
HTTP Request Dependency Graph 50
HTTP Packets 50
SMTP Packets 51
Code Manipulations 54
Statistics 54
Behavior 54
System Behavior 54
Analysis Process: SW0P9o9ksjpBsnr.exe PID: 5468 Parent PID: 6036 54
General 54
File Activities 55
File Created 55
File Written 55
File Read 55
Analysis Process: BackgroundTransferHost.exe PID: 4928 Parent PID: 792 55
General 55
File Activities 55
Analysis Process: SW0P9o9ksjpBsnr.exe PID: 4928 Parent PID: 5468 56
General 56
File Activities 58
File Created 58
File Written 58
Analysis Process: bin.exe PID: 6480 Parent PID: 4928 58
General 58
File Activities 60
File Created 60
File Read 60
Registry Activities 60
Key Created 60
Key Value Created 60
Analysis Process: warz.exe PID: 6544 Parent PID: 4928 60
General 60
File Activities 62
File Created 62
File Written 62
File Read 62
Registry Activities 62
Key Created 62
Key Value Created 62
Key Value Modified 62
Analysis Process: rem.exe PID: 6564 Parent PID: 4928 62
General 62
File Activities 63
File Created 63
Registry Activities 63
Key Created 63
Key Value Created 63
Analysis Process: powershell.exe PID: 6572 Parent PID: 6480 63
General 63
File Activities 63
File Created 63
File Deleted 63
File Written 63
File Read 63
Analysis Process: cmd.exe PID: 6580 Parent PID: 6480 63
General 63
Analysis Process: conhost.exe PID: 6588 Parent PID: 6572 64
General 64
Analysis Process: conhost.exe PID: 6596 Parent PID: 6580 64
General 64
Analysis Process: powershell.exe PID: 6764 Parent PID: 6544 64
General 64
Analysis Process: hawkstartup.exe PID: 6776 Parent PID: 4928 65
General 65
Analysis Process: conhost.exe PID: 6808 Parent PID: 6764 66
General 66
Analysis Process: images.exe PID: 6824 Parent PID: 6544 66
General 66
Analysis Process: ori4.0dec23sta.exe PID: 6988 Parent PID: 4928 69
General 69
Analysis Process: powershell.exe PID: 7092 Parent PID: 6824 69
General 69
Analysis Process: ori2.0dec23sta.exe PID: 7112 Parent PID: 4928 70
General 70
Disassembly 71
Code Analysis 71

Copyright Joe Security LLC 2022

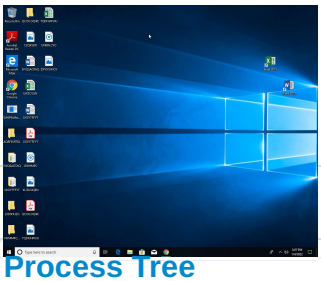
Windows Analysis Report SW0P9o9ksjpBsnr.exe

Overview

General Information

Sample Name:	SW0P9o9ksjpBsnr.exe
Analysis ID:	547727
MD5:	27f2a9688ec34fc..
SHA1:	9464f6bea3222c5.
SHA256:	5733ad0577f5b8f..
Tags:	exe RemcosRAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

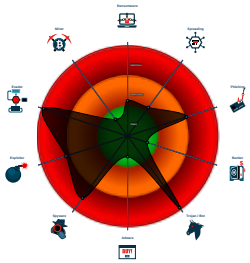
HawkEye Remcos AgentTesla AveMaria MailPassView UACMe

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Yara detected UACMe UAC Bypass…
- Detected HawkEye Rat
- Yara detected AveMaria stealer
- Detected Remcos RAT

Classification



Process Tree

- **System is w10x64**
- SW0P9o9ksjpBsnr.exe (PID: 5468 cmdline: "C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe" MD5: 27F2A9688EC34FC8AA3B0FEE4757DD71)
  - BackgroundTransferHost.exe (PID: 4928 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
    - bin.exe (PID: 6480 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" 0 MD5: 805FBB84293E86F25B566A5B2C2815D2)
      - powershell.exe (PID: 6572 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 6588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6580 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - warz.exe (PID: 6544 cmdline: "C:\Users\user\AppData\Local\Temp\warz.exe" 0 MD5: 1D90A7DA17807F64F1699E5EA2091A36)
      - powershell.exe (PID: 6764 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 6808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - images.exe (PID: 6824 cmdline: C:\ProgramData\images.exe MD5: 1D90A7DA17807F64F1699E5EA2091A36)
        - powershell.exe (PID: 7092 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 7156 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rem.exe (PID: 6564 cmdline: "C:\Users\user\AppData\Local\Temp\rem.exe" 0 MD5: 9E764165FBA9E86937643D84A2F4E063)
    - hawkstartup.exe (PID: 6776 cmdline: "C:\Users\user\AppData\Local\Temp\hawkstartup.exe" 0 MD5: AEAF1943FB037B6529873D7CC47CE137)
      - Windows Update.exe (PID: 3328 cmdline: "C:\Users\user\AppData\Roaming\Windows Update.exe" MD5: AEAF1943FB037B6529873D7CC47CE137)
        - dw20.exe (PID: 5040 cmdline: dw20.exe -x -s 2228 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
        - vbc.exe (PID: 1456 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: 4692 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
        - WerFault.exe (PID: 1896 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3328 -s 2232 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - WerFault.exe (PID: 4600 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3328 -s 2232 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - ori4.0dec23sta.exe (PID: 6988 cmdline: "C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe" 0 MD5: F41809BC71EEB2C3B1676309139216A8)
    - ori2.0dec23sta.exe (PID: 7112 cmdline: "C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe" 0 MD5: 421138225D5DEE81805C5E5072898504)
    - BackgroundTransferHost.exe (PID: 6776 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
  - SW0P9o9ksjpBsnr.exe (PID: 4928 cmdline: C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe MD5: 27F2A9688EC34FC8AA3B0FEE4757DD71)
- bin.exe (PID: 7136 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: 805FBB84293E86F25B566A5B2C2815D2)
- WindowsUpdate.exe (PID: 6840 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: AEAF1943FB037B6529873D7CC47CE137)
- 100.exe (PID: 5772 cmdline: "C:\Users\user\AppData\Roaming\100\100.exe" MD5: F41809BC71EEB2C3B1676309139216A8)
- WindowsUpdate.exe (PID: 7164 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: AEAF1943FB037B6529873D7CC47CE137)
- 100.exe (PID: 6576 cmdline: "C:\Users\user\AppData\Roaming\100\100.exe" MD5: F41809BC71EEB2C3B1676309139216A8)
- **cleanup**

Copyright Joe Security LLC 2022

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\100\100.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Roaming\100\100.exe	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
C:\ProgramData\images.exe	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
C:\ProgramData\images.exe	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:
C:\ProgramData\images.exe	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x144e8:$a1: \Opera Software\Opera Stable\Login Data • 0x14810:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14158:$a3: \Google\Chrome\User Data\Default\Login Data

Click to see the 36 entries

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000003.295733640.00000000010D3000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000B.00000003.295733640.00000000010D3000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000017.00000000.312592775.00000000008C2000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000000.312592775.00000000008C2000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001F.00000002.435763826.00000000081E0000.00000004.00020000.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df

Click to see the 376 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
22.3.images.exe.14b3768.4.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xb18:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
22.3.images.exe.14b3768.4.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xb18:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xb18:$c1: Elevation:Administrator!new:
22.3.images.exe.14b3768.4.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
22.3.images.exe.14b4d00.6.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
22.3.images.exe.14b4d00.6.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:

Click to see the 584 entries

Sigma Overview

System Summary:

Copyright Joe Security LLC 2022

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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 Remcos RAT

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits:

Yara detected UACMe UAC Bypass tool

Networking:

Connects to many ports of the same IP (likely port scanning)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected Remcos RAT

Yara detected AveMaria stealer

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates autostart registry keys with suspicious names

Copyright Joe Security LLC 2022

Hooking and other Techniques for Hiding and Protection:

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

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

.NET source code references suspicious native API functions

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Yara detected AgentTesla

Yara detected Remcos RAT

Yara detected AveMaria stealer

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

Contains functionality to steal e-mail passwords

Yara detected WebBrowserPassView password recovery tool

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

Yara detected HawkEye Keylogger

Yara detected AgentTesla

Yara detected Remcos RAT

Detected HawkEye Rat

Yara detected AveMaria stealer

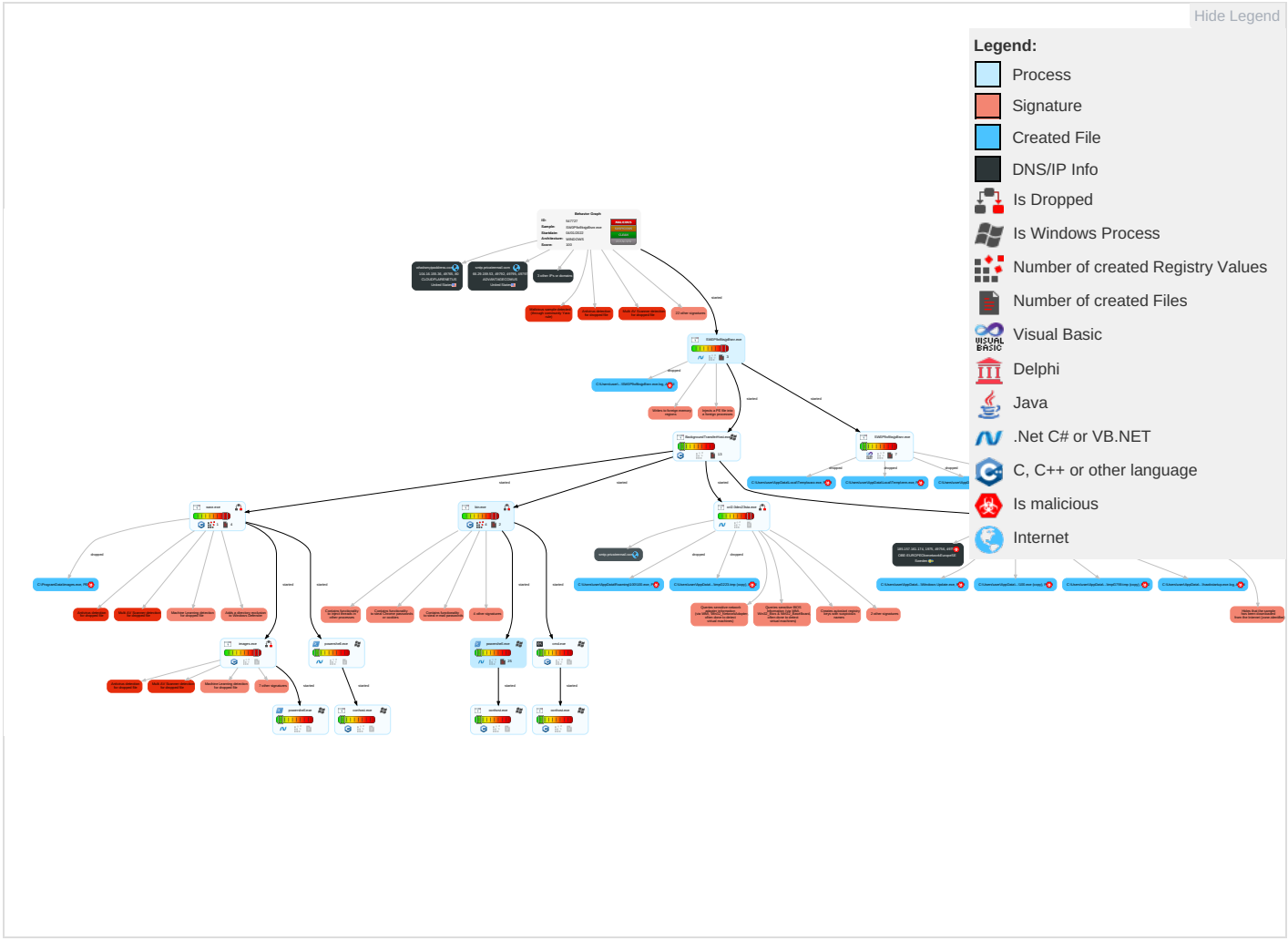
Detected Remcos RAT

Mitre Att&ck Matrix

Copyright Joe Security LLC 2022

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 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1	OS Credential Dumping 3	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 2	Exfiltration Over Network Mediur
Default Accounts	Native API 2 1	Create Account 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1 3 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Windows Service 1	Windows Service 1	Obfuscated Files or Information 3 1	Credentials In Files 1	System Service Discovery 1	SMB/Windows Admin Shares	Input Capture 1 3 1	Automated Exfil
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 1 1	Process Injection 5 2 2	Software Packing 1 1	NTDS	File and Directory Discovery 3	Distributed Component Object Model	Clipboard Data 1	Scheduled Trar
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1 1	DLL Side-Loading 1	LSA Secrets	System Information Discovery 1 2 4	SSH	Keylogging	Data Transfer S Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 3	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Security Software Discovery 3 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Prot
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encr Non-C2 Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 2 2	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Enc Non-C2 Protocc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Ob Non-C2 Protocc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Users 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Mediur
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over

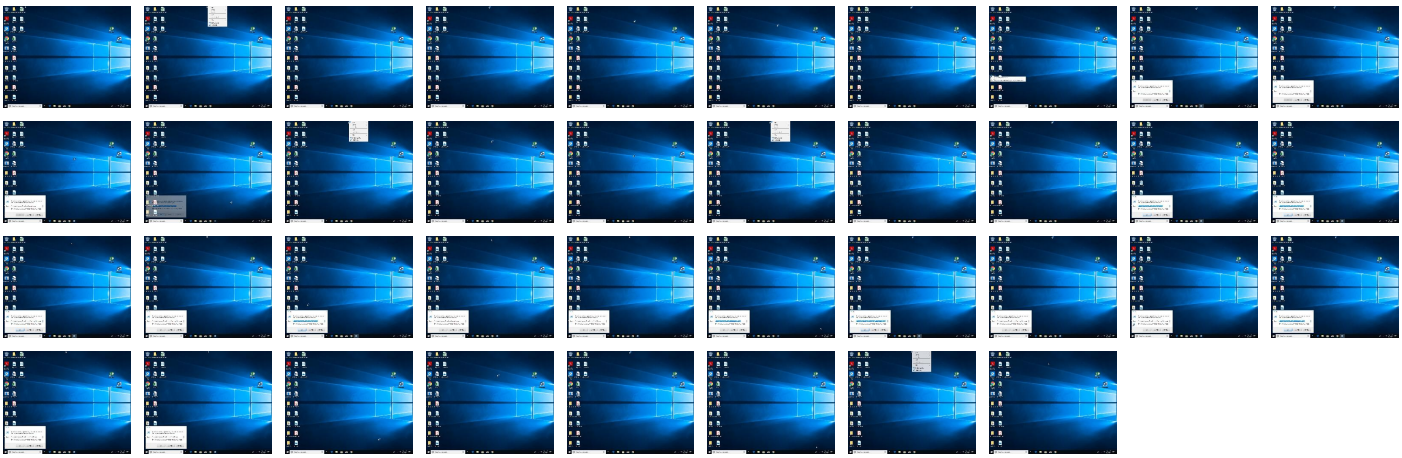
Behavior Graph



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
SW0P9o9ksjpBsnr.exe	53%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SW0P9o9ksjpBsnr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\100\100.exe	100%	Avira	TR/Spy.Gen8	
C:\ProgramData\images.exe	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\warz.exe	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\hawkstartup.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Local\Temp\hawkstartup.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe	100%	Avira	TR/Spy.Gen8	
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\Roaming\100\100.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\warz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\hawkstartup.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\rem.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	76%	Metadefender		Browse
C:\ProgramData\images.exe	89%	ReversingLabs	Win32.Backdoor.Remcos	
C:\Users\user\AppData\Local\Temp\bin.exe	76%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bin.exe	89%	ReversingLabs	Win32.Backdoor.Remcos	
C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe	51%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\rem.exe	50%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\rem.exe	86%	ReversingLabs	Win32.Trojan.Remcos	
C:\Users\user\AppData\Local\Temp\tmpG223.tmp (copy)	86%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Local\Temp\tmpG759.tmp (copy)	51%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\tmpG759.tmp (copy)	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\warz.exe	76%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\warz.exe	89%	ReversingLabs	Win32.Backdoor.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.warz.exe.1020000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
26.0.ori2.0dec23sta.exe.d0000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
12.2.warz.exe.1020000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
19.0.hawkstartup.exe.4d0000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
19.0.hawkstartup.exe.4d0000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
22.0.images.exe.330000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
11.0.bin.exe.880000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
26.0.ori2.0dec23sta.exe.d0000.2.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.8.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.8.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.bin.exe.880000.2.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
22.3.images.exe.14ab2f0.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
11.0.bin.exe.880000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
19.0.hawkstartup.exe.4d0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
19.0.hawkstartup.exe.4d0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.bin.exe.880000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
22.2.images.exe.330000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
19.0.hawkstartup.exe.4d0000.12.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
19.0.hawkstartup.exe.4d0000.12.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
26.0.ori2.0dec23sta.exe.d0000.1.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
4.2.SW0P9o9ksjpBsnr.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.2.SW0P9o9ksjpBsnr.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.2.SW0P9o9ksjpBsnr.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.2.SW0P9o9ksjpBsnr.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.2.SW0P9o9ksjpBsnr.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.3.images.exe.14ab2f0.10.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
19.0.hawkstartup.exe.4d0000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
19.0.hawkstartup.exe.4d0000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.SW0P9o9ksjpBsnr.exe.3e95f28.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.ori4.0dec23sta.exe.8c0000.1.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.2.bin.exe.880000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.12.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.12.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.12.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.12.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.0.SW0P9o9ksjpBsnr.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.ori4.0dec23sta.exe.8c0000.3.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
23.2.ori4.0dec23sta.exe.8c0000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
26.2.ori2.0dec23sta.exe.d0000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
23.0.ori4.0dec23sta.exe.8c0000.2.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
19.2.hawkstartup.exe.4d0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
19.2.hawkstartup.exe.4d0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
12.0.warz.exe.1020000.2.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
23.0.ori4.0dec23sta.exe.8c0000.0.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
26.0.ori2.0dec23sta.exe.d0000.3.unpack	100%	Avira	HEUR/AGEN.1143187		Download File
12.0.warz.exe.1020000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
12.0.warz.exe.1020000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://hWWJFF.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://KXOf8Lcd51drIxRwI.orgd=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://KXOf8Lcd51drIxRwI.org	0%	Avira URL Cloud	safe	
http://www.tiro.com2	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.tiro.comB	0%	Avira URL Cloud	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://https://KXOf8Lcd51drIxRwI.org81	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.monotypeimaging.c	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comslnt	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comAt	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://KXOf8Lcd51drIxRwI.orgInProcServer32	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crl.c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://KXOf8Lcd51drIxRwI.orgInprocHandler	0%	Avira URL Cloud	safe	
http://CDIeMO.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceaY	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
smtp.privateemail.com	66.29.159.53	true	false		high
9.96.11.0.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
185.157.161.174	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
66.29.159.53	smtp.privateemail.com	United States		19538	ADVANTAGECOMUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	547727
Start date:	04.01.2022

Copyright Joe Security LLC 2022

Start time:	15:04:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SW0P9o9ksjpBsnr.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:	50
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winEXE@46/115@17/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.9% (good quality ratio 24.8%) • Quality average: 79% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 64% • 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
15:05:49	API Interceptor	1x Sleep call for process: SW0P9o9ksjpBsnr.exe modified
15:06:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Images C:\Users\user\AppData\Local\Temp\bin.exe
15:06:05	API Interceptor	91x Sleep call for process: rem.exe modified
15:06:06	API Interceptor	111x Sleep call for process: powershell.exe modified
15:06:08	API Interceptor	1592x Sleep call for process: cmd.exe modified
15:06:24	API Interceptor	424x Sleep call for process: ori2.0dec23sta.exe modified
15:06:24	API Interceptor	21x Sleep call for process: Windows Update.exe modified
15:06:27	API Interceptor	567x Sleep call for process: ori4.0dec23sta.exe modified
15:06:27	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
15:06:35	API Interceptor	1x Sleep call for process: dw20.exe modified
15:06:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 100 C:\Users\user\AppData\Roaming\100\100.exe
15:06:44	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
15:06:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 100 C:\Users\user\AppData\Roaming\100\100.exe
15:06:59	API Interceptor	233x Sleep call for process: 100.exe modified
15:07:03	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

Copyright Joe Security LLC 2022

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\images.exe	
Process:	C:\Users\user\AppData\Local\Temp\warz.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.3755741620209365
Encrypted:	false
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE01Ne:K1VmhaH8EFvW+0OVE0f
MD5:	1D90A7DA17807F64F1699E5EA2091A36
SHA1:	94BC36E1791CF32A00CBCED56BBC26B9FCDB83BC
SHA-256:	1B7C4871410C1AF15640CF7524EB887EF4AA416027B727FE6D32ED48DAD03A5E
SHA-512:	5592D140691F092AD46D38FC1A635D1F5206A796180146894AEE0FE2101D957F4BFFA0CE968A5E074182D2CBAAB9903E67413A06CD9CC54C112220E77A555F98
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\ProgramData\images.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 76%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3.?<..7D..?<...3.<<.....?<.....=<..;0..?<..7D..:<..7D..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....PE..L.....I_.....0.....\.....@....@.....@.....@.....w.....p,..... .....u..... .....@..p.....text.....0..... ..`.rdata...I...@...J...4.....@..@.data....P.....~.....@....rsrc...p,.....@..@.reloc..... .....@..B.bss.....0.....@..@.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hawkstartup.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\hawkstartup.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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hawkstartup.exe.log	
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\Microsoft\CLR_v4.0_32\UsageLogs\SW0P9o9ksjpBsnr.exe.log	
Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22368
Entropy (8bit):	5.603645337088908
Encrypted:	false
SSDEEP:	384:HtCDhhikbvV/K/SZO090C+RcS0nkjultli/7Y9gxSJ3xST1MaDZlbAV7LjUQZu5M:ClK/SQYjTkCltd7xcgCSfwf0Vk
MD5:	991B2C2382791C58F60FAEA90A28C248
SHA1:	0859021B1C373C875CA0EC5C5D4EF6176E3E1F63
SHA-256:	D97E42F64A7686C8E3B0730F5B227229B50A9BD43ECF277363F0FFB0E3BC660E
SHA-512:	8DCEE70DF93E1CAD9165260A467FA10BA1EFF8A1BE8AEEE2D5623BB832B430E54FAD9D09DFC076B3393305C59BA6063C9E0582CE554B48FD24FC4A2EB660FBBF
Malicious:	false
Reputation:	unknown
Preview:	@...e.....h.....J.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Process:	C:\Users\user\AppData\Local\Temp\hawkstartup.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.328367439558377
Encrypted:	false
SSDEEP:	3:oNUkh4E2J5xAI4LyJ:oN923f4yJ
MD5:	0E653EA1CA5B51AE6B0407A3B06ABDB2
SHA1:	3215A0FB9DFF9E5206F4EA532083883667CCA1B2
SHA-256:	342B658E9D2BF4EC676BE1E0825D358E795FB25EC950181226160D8D59A4A348
SHA-512:	8E5550682036905321BDFB687C1A85453D1316633816126CEB9EA3140C79E25B606581457893AEC666D22DC97467345EE02E901AF8B0E571C2B07B883A459917

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\hawkstartup.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4rgqrzb1.mio.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eu3ejk2l.dei.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_f30gmf23.2tk.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jhvqfjsx.lnn.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jhvqfjsx.lnn.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ssu14o0g.t05.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_who4ph3w.f4y.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\bin.exe	
Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.375962866007663
Encrypted:	false
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE01:K1VmhaH8EFvW+0OVE0
MD5:	805FBB84293E86F25B566A5B2C2815D2
SHA1:	5712F69EAFCA434E4D6CDFD8081EBFB728708C25
SHA-256:	E78FCD503A6B0A663AB4A72B97C010C932840998DA05784BA75F7D6802EA822F
SHA-512:	5927584ABABC4C2D533984C607A96590D1640B6939D33E9F994B684F38F1541DFDC1D0778F5DBE586353C46BEBC3A7F0E46A1156F34E5748AB31FF0AF16807A2
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: unknown

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

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 76%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3.?<..7D..?<...3.<<.....?<.....=<..;0..?<..7D..:<..7D..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....PE..L.....I_.....0.....\.....@....@.....@.....@.....w.....p,..... .....u..... .....@..p.....text.....0..... ..`.rdata...I...@...J...4.....@..@.data....P.....~.....@....rsrc...p,.....@.@.reloc..... .....@..B.bss.....0.....@..@..... .....

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

Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	532992
Entropy (8bit):	6.50689182620986
Encrypted:	false
SSDEEP:	6144:XujqWRdUbS/QTjhUqBfxrwEnuNcSsm7IoYGW0VvBXCAt6kihwE+VDpJYWmlwnx9w:IdUQtqB5urTIoYWBQk1E+VF9mOx9wi
MD5:	AEAF1943FB037B6529873D7CC47CE137
SHA1:	146F9F3451B53A95C7783903C522EC873AE05B80
SHA-256:	D28142C344D44B16AD7B4B0FB8634B2AD3BF8638BC001CDDC3872B5892B01DF1
SHA-512:	1DDAA2CD43597B8B25E609113FC005B6CD8384B40197731E7BD8DEB182A94493B741726867849594979FBF7E983EEDC1532016E7C26D54DCA573585B1B8871CA
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.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\hawkstartup.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.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...J..a.....4..... .....@.. ....@.....X...S.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.rel oc.....`..... .....@..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.....*.R..(....o....o.....

C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe

Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	220672
Entropy (8bit):	6.055847125653901
Encrypted:	false
SSDEEP:	3072:LVQD9iZkWDVXgc5YOoNUJtJRzRM34QoZaexsVw3Ny5PSv4+ckvDXZFNVQYUygYj:Licg5UHNMAZTsYyEv4+hLZh1U
MD5:	421138225D5DEE81805C5E5072898504
SHA1:	2FF010EA34F2967839B35BE9F60D95AAD4BA73D1
SHA-256:	E2B9FA401F76BAB3AC4E4121DA34804699A143F3F8DF13E4BA14885671EB2804
SHA-512:	5C1CFBA4446BFF8BE8CA0345C60D74685E08991FC316E89B705EFAB65B9E066D540E7D75C781736ECDD6FF4AA0900BF73B8463218AAC378BEB02D7B12B43473A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....V.....Nt... .....@.. ....@.....s..O..... ....H.....text...TT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....\.....@..B.....0t.....H.....T.....(....*..(....*.s.....s.....s.....s.....*...0.....+.....,.....,.....,.....,.+.+.~....o....*.0 ..,.....+.....,.....,.....,.+.+.~....o....*.0.,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(..... +.....,.....,.....,.+.+..(....*.0.,.....

C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe	
Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.0611591430910705
Encrypted:	false
SSDEEP:	3072:h9W62gdD+uiigULgEVbF2nAbTIAfdXUiuC4kQdMDfS0RyCdMjVwuNyqrs8SnKV3i:hyCanArxULLdmHunyp8SKxzal6GTC
MD5:	F41809BC71EEB2C3B1676309139216A8
SHA1:	C012A5FFB060A5B841D17D6BB82602D01364901C
SHA-256:	7E6D00EB0D8DA711EAD4C519CA281C294066BC3BC2146EB62918998AE3C54E34
SHA-512:	F27FE07EEAA7CC1FC622631404F8A30F7C81FB804765788C6CEE43FE72EF0F10717CE654DD1F2A1A928177E3168B69136A6B9CBE05EE4C83034D8C9940728FB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..a.....V.....>u... .....@.. ....@.....t..K..... ....H.....text...DU... ...V..... ..`.rsrc... .....X.....@..@.rel oc.....^.....@..B..... u.....H.....(....*..(....*.s.....s.....s.....s.....*...0.,.....+.....,.....,.....,.+.+.~....o....*.0. .,.....+.....,.....,.....,.+.+.~....o....*.0.,.....+.....,.....,.....,.+.+.~....o....*.0.,.....+.....,.....,.....,.+.+..(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0.,.....

C:\Users\user\AppData\Local\Temp\rem.exe	
Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	474112
Entropy (8bit):	6.5805818899521675
Encrypted:	false
SSDEEP:	12288:iegN0jfYLclGb0bVT6e+MT2MffZS/gzSYo:ENywLclGIeMT2MXZRzSV
MD5:	9E764165FBA9E86937643D84A2F4E063
SHA1:	0AACD8A74DE058034C1B9224F8CD82E5B7D07102
SHA-256:	DD925001A61D7D233BF538D891975F242E205FF1A40935332076BF85FCDE6271
SHA-512:	3AA4E36FF823CBA55737464FDFA85B1195A86BE36265FCF05EBE3B28DE3510FE3AE79C14F1DEB21B26C599D643ADE5B7230E822E849476E655883FDBA314568
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\rem.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\rem.exe, Author: unknown
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 50%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}4V..gV..gV..g...gD..g...g...g...gH..g_.gW..g.<.gT..gm..fL.. gm..fl..gm..ft..g_.gC..gV..g...g...f...g...gW..g...fW..gRichV..g.....PE..L...s..a.....,.....r.....@....@..... ...K..... ...p..49.. }..8.....}.....X}..@.....@.....text....+.....,..... ..`.rdata...p...@...r...0.....@..@.data....>.....@....tls..... .....@....gfids..0.....@..@.rsrc....K... ...L.....@..@.reloc..49...p...:.....@..B.....

C:\Users\user\AppData\Local\Temp\tmpG223.tmp (copy)	
Process:	C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:LVQD9iZkWDVXgc5YOoNUJtJRzRM34QoZaexsVw3Ny5PSv4+ckvDXZFNVQYUygYj:Licg5UHNMAZTsYyEv4+hLZh1U
MD5:	421138225D5DEE81805C5E5072898504
SHA1:	2FF010EA34F2967839B35BE9F60D95AAD4BA73D1
SHA-256:	E2B9FA401F76BAB3AC4E4121DA34804699A143F3F8DF13E4BA14885671EB2804
SHA-512:	5C1CFBA4446BFF8BE8CA0345C60D74685E08991FC316E89B705EFAB65B9E066D540E7D75C781736ECDD6FF4AA0900BF73B8463218AAC378BEB02D7B12B43473 A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmpG223.tmp (copy)

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....V.....Nt... .....@.. ....@.....s..O..... ....H.....text...TT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....\.....@..B.....0t.....H.....T.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0 ..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(..... +.....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\tmpG759.tmp (copy)

Process:	C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.0611591430910705
Encrypted:	false
SSDEEP:	3072:h9W62gdD+uiigULgEVbF2nAbTIAfdXUiuC4kQdMDfS0RyCdMjVwuNyqrs8SnKV3i:hyCanArxULLdmHunyp8SKxzal6GTC
MD5:	F41809BC71EEB2C3B1676309139216A8
SHA1:	C012A5FFB060A5B841D17D6BB82602D01364901C
SHA-256:	7E6D00EB0D8DA711EAD4C519CA281C294066BC3BC2146EB62918998AE3C54E34
SHA-512:	F27FE07EEAA7CC1FC622631404F8A30F7C81FB804765788C6CEE43FE72EF0F10717CE654DD1F2A1A928177E3168B69136A6B9CBE05EE4C83034D8C9940728FB
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..a.....V.....>u... .....@.. ....@.....t..K..... ....H.....text...DU... ...V..... ..`.rsrc... .....X.....@..@.rel oc.....^.....@..B..... u.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0. ..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+...(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0..,.....

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

Process:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.3755741620209365
Encrypted:	false
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE01Ne:K1VmhaH8EFvW+0OVE0f
MD5:	1D90A7DA17807F64F1699E5EA2091A36
SHA1:	94BC36E1791CF32A00CBCED56BBC26B9FCDB83BC
SHA-256:	1B7C4871410C1AF15640CF7524EB887EF4AA416027B727FE6D32ED48DAD03A5E
SHA-512:	5592D140691F092AD46D38FC1A635D1F5206A796180146894AEE0FE2101D957F4BFFA0CE968A5E074182D2CBAAB9903E67413A06CD9CC54C112220E77A555F98
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 76%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3.?<..7D..?<...3.<<.....?<.....=<..;0..?<..7D..:<..7D..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....PE..L.....I_.....0.....\.....@....@.....@.....@.....w.....p,.....u..... .....@..p.....text.....0..... ..`.rdata...I...@...J...4.....@..@.data....P.....~.....@....rsrc...p,.....@. .@.reloc..... .....@..B.bss.....0.....@..@.....

C:\Users\user\AppData\Roaming\100\100.exe

Process:	C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:h9W62gdD+uiigULgEVbF2nAbTIAfdXUiuC4kQdMDfS0RyCdMjVwuNyqrs8SnKV3i:hyCanArxULLdmHunyp8SKxzal6GTC

C:\Users\user\AppData\Roaming\100\100.exe	
MD5:	F41809BC71EEB2C3B1676309139216A8
SHA1:	C012A5FFB060A5B841D17D6BB82602D01364901C
SHA-256:	7E6D00EB0D8DA711EAD4C519CA281C294066BC3BC2146EB62918998AE3C54E34
SHA-512:	F27FE07EEAA7CC1FC622631404F8A30F7C81FB804765788C6CEE43FE72EF0F10717CE654DD1F2A1A928177E3168B69136A6B9CBE05EE4C83034D8C9940728FB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\100\100.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\100\100.exe, Author: Joe Security
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.....V.....>u... .....@.. ....@.....t..K..... ....H.....text...DU... ...V..... ..`.rsrc... .....X.....@..@.rel oc.....^.....@..B..... u.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0. .,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Roaming\100\100.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.0611591430910705
Encrypted:	false
SSDEEP:	3072:h9W62gdD+uiigULgEVbF2nAbTIAfdXUiuC4kQdMDfS0RyCdMjVwuNyqrs8SnKV3i:hyCanArxULLdmHunyp8SKxzal6GTC
MD5:	F41809BC71EEB2C3B1676309139216A8
SHA1:	C012A5FFB060A5B841D17D6BB82602D01364901C
SHA-256:	7E6D00EB0D8DA711EAD4C519CA281C294066BC3BC2146EB62918998AE3C54E34
SHA-512:	F27FE07EEAA7CC1FC622631404F8A30F7C81FB804765788C6CEE43FE72EF0F10717CE654DD1F2A1A928177E3168B69136A6B9CBE05EE4C83034D8C9940728FB
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..a.....V.....>u... .....@.. ....@.....t..K..... ....H.....text...DU... ...V..... ..`.rsrc... .....X.....@..@.rel oc.....^.....@..B..... u.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~....o....*.0. .,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0..(.....+ .....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_150604.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794025
Entropy (8bit):	7.943882793165034
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+M:ZSiGvxfK7ZMWSFpC6p8FE/Qq//H
MD5:	D4EB61682F95D08DFC9567306B5C9B16
SHA1:	34A411C597C5774E7982E344BF1420F34F5ABAA6
SHA-256:	C23663D85A5FCEB40BFE6DC6BDB316DD71D200947DED160ABB69C616A876541E
SHA-512:	44F44C55D416D6650E0EBBB9F0F51A5D93633545F48CD997744446F39E93386021054465523B3B9AE231BAC0EA407062417CAD59E5E68885BA5C793243DCA758
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[}x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_151605.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794030
Entropy (8bit):	7.9439270855102535
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+3:ZSiGvxfK7ZMWSFpC6p8FE/Qj29n+
MD5:	50E6CD211911C31C62D4B423DB6E9AB5
SHA1:	6820D4090D87DF1E352CE7D16389A032DAEBFF4A

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_151605.png	
SHA-256:	5039764FD5E0567D1730317580C3EBFEEB7B17BC7E52F2CD24BEF8AF68774B90
SHA-512:	D2FC1719A0B8C8BD6137D51A46960A10036C029DD9E82B7DCBE82D13209D36AF46F119F1B762E85E408E376BA643446E104912EE0A4C3E929BB900EEDA5228B
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_152610.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794683
Entropy (8bit):	7.944435033884138
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//funJ:ZSiGvxfK7ZMWSFpC6p8FE//fuKkhCjg/
MD5:	7AE836421A27084740BFF84057CB37DA
SHA1:	DA2AD34E16A411976EAB29F30DA2E38D347D8B7C
SHA-256:	E4B46D63A37A05D9028A7CF6CE2293441F42051B3D0225714CE9326CB3619872
SHA-512:	8AA4F8B5B64D2C167791BE6D8A90F569A78737E41AAC543BA9A1DFA44D332E13019C46E197246C09C2D59A9340C78A152FB4DAF725A1AE18D02846EA7F11CFE D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_153610.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794683
Entropy (8bit):	7.944435033884138
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//funJ:ZSiGvxfK7ZMWSFpC6p8FE//fuKkhCjg/
MD5:	7AE836421A27084740BFF84057CB37DA
SHA1:	DA2AD34E16A411976EAB29F30DA2E38D347D8B7C
SHA-256:	E4B46D63A37A05D9028A7CF6CE2293441F42051B3D0225714CE9326CB3619872
SHA-512:	8AA4F8B5B64D2C167791BE6D8A90F569A78737E41AAC543BA9A1DFA44D332E13019C46E197246C09C2D59A9340C78A152FB4DAF725A1AE18D02846EA7F11CFE D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_154611.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794683
Entropy (8bit):	7.944435033884138
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//funJ:ZSiGvxfK7ZMWSFpC6p8FE//fuKkhCjg/
MD5:	7AE836421A27084740BFF84057CB37DA
SHA1:	DA2AD34E16A411976EAB29F30DA2E38D347D8B7C
SHA-256:	E4B46D63A37A05D9028A7CF6CE2293441F42051B3D0225714CE9326CB3619872
SHA-512:	8AA4F8B5B64D2C167791BE6D8A90F569A78737E41AAC543BA9A1DFA44D332E13019C46E197246C09C2D59A9340C78A152FB4DAF725A1AE18D02846EA7F11CFE D
Malicious:	false

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_154611.png	
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_155617.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_160618.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_161618.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_162619.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..  M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_163620.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..  M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_164620.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..  M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_165621.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_165621.png	
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_170621.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_171622.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_172623.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_172623.png	
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_173623.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_174624.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_175625.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	801724
Entropy (8bit):	7.94317946801279
Encrypted:	false
SSDEEP:	12288:UNGZS9+Wp0T9e4Lm8504VFeerXxR4WnQDnX5qKHaG1uVuOOMg:L6+WC9H504NR404oKHayOOr
MD5:	F461190699F2E3869CC1C766851E93A5
SHA1:	41F8EB6AB8A70AF682765602D1EC1FF80A9A3F99
SHA-256:	DE0F627C7C6FD648FDD15C4A5EB710F42E9A64EDD7D8E6FE83B43F3C8926EE6A
SHA-512:	46C6764F9D1428145FB29FFDAB17CBF96D81E56A9871EEB73D7A271CC2DFFC80DD6A19647F9C59193F55F721E489E7568B29F6C4DFFD5F8EDEB36AE19A889F D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_175625.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....Fy...17.K'..._.N1.....\L.\.H!..B..L(....1..4..jlz16=$..C..)..t..66.?.H..o.....j..y_.....]if4.I3.\|..... ....k.Q.....m7....{.7iem..F..y.2..y..[D....-k.i..V..s...o...I....b..y7.~=..k.o6cO.....\...vm..b....g}..u.Zp..9.Xn....K3....~6.}....{.'.[.,..._.v..n./HSG....4.Ge....=....p...n.{.u.%".....-.<..... .\.l..e..{6.{a..b.r.`.....:n.....:n.....?l64FqDc.....b.....j.....n...PK\.....}o..._.+_.....s.5...>.u<.....O."....X.....h.7.}x..#=.,.=.\|R....R.\H..Q..c...O..{.u...'..5..q...M.e.X.....8.B.v...XZ...f.. {...4.=9';.x.S.q4..n .,@ .OP.h;>....1D...UJ&.x2.qBu..o..y.....E...[...&.8..6.H..d{f=.I..0...@c.G2.....c.....?....N.$..C.....^4...><..[.,....3X[.,m.m...}.3..6.....,.+.u}..g[h.....K.`y....p..U.. Nh".'..>..Fm.n.....t.2.#(...6..L....tls.,v~.= z<.I.i.` +..S..O&vB....6...Z....>v.. .....xQ.4u.B....]..`..*.T.m.....:.....+s(.?)..E..].....

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_180625.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810256
Entropy (8bit):	7.944174173318863
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcZvCSvP:QDfLWE/b8D/vP
MD5:	2BA8EC6BC5415D932D8C2306FA8F9CF7
SHA1:	6409E0F33958EA38B12DD23430CCA4745BE51127
SHA-256:	9546F04506AD850EA65E7707EA6B5FA2DA579AF43D9C5D98071FADB9C05958AE
SHA-512:	6F2476A7F72CEF8157174F0A64BF44D8C30B70980435810499ECD6AF54AA858DBE56D94A6D17BEC99790865B1769018DEA57CBF2F2519EC31B7C60A2DC465BC
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_181626.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795129
Entropy (8bit):	7.943552777920506
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+F:ZSiGvxfK7ZMWSFpC6p8FE/Q9Ima9SeW
MD5:	ECAEA4C6C9CC78C158033127BE390B5C
SHA1:	41EECC4A1C94F22C32ECFA8036A691D9F076E314
SHA-256:	39AD908A3F20BD925E7EFA84299B39AEAEC13527F09652FA3050A681C55A16E1
SHA-512:	A4D0574B8844D22DD51B668426110409DF6246C330FCBCCEBB331DBE6517BAF52C79774A754B641807C417CDDD9336C02E4DB93E00D0EF7F375AB228AE132A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_182626.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795129
Entropy (8bit):	7.943552777920506
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+F:ZSiGvxfK7ZMWSFpC6p8FE/Q9Ima9SeW
MD5:	ECAEA4C6C9CC78C158033127BE390B5C
SHA1:	41EECC4A1C94F22C32ECFA8036A691D9F076E314
SHA-256:	39AD908A3F20BD925E7EFA84299B39AEAEC13527F09652FA3050A681C55A16E1
SHA-512:	A4D0574B8844D22DD51B668426110409DF6246C330FCBCCEBB331DBE6517BAF52C79774A754B641807C417CDDD9336C02E4DB93E00D0EF7F375AB228AE132A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_183627.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795129
Entropy (8bit):	7.943552777920506
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+F:ZSiGvxfK7ZMWSFpC6p8FE/Q9Ima9SeW
MD5:	ECAEA4C6C9CC78C158033127BE390B5C
SHA1:	41EECC4A1C94F22C32ECFA8036A691D9F076E314
SHA-256:	39AD908A3F20BD925E7EFA84299B39AEAEC13527F09652FA3050A681C55A16E1
SHA-512:	A4D0574B8844D22DD51B668426110409DF6246C330FCBCCEBB331DBE6517BAF52C79774A754B641807C417CDDD9336C02E4DB93E00D0EF7F375AB228AE132A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;..,|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_184628.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795096
Entropy (8bit):	7.943681228415246
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+h:ZSiGvxfK7ZMWSFpC6p8FE/QogJN
MD5:	D1B697D6D5117278C21A270C3248DAFC
SHA1:	0C635068F7FB5193F023B700F0C2C985B239EEAB
SHA-256:	228504CE2AC4BD91D80675E2816344FFBB6EE3E1617D28E0D70541D8CA58B581
SHA-512:	BDEE909F839572CBDBD82E3B2C1D09CFD84B022659A86E5D6BCFB42FC65E3B55C80835A93D6C103CC4C0B3E539BEC2C674A2408ACBD8F1989FBC98A35FF04 61
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;..,|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_185631.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795281
Entropy (8bit):	7.943729813452789
Encrypted:	false
SSDEEP:	24576:ZSiGvxfK7ZMWSFpC6p8FE/QdNrsIcsSea:QDfLWE/QDrsIczea
MD5:	6793E87EFA493F5299239C64B60A1E22
SHA1:	4BE29C82FF5CF58B5B11975326792610B3374414
SHA-256:	A3BD151A1CDF1F911B72E3001676DB680773519BFB42C5C8F3D756CECE92FB70
SHA-512:	E8096C3D6981570D97DC14E7C4A839EF5482E9335A5FBE66AD4EAC1957AB6FFDE6B199968449700F6554478EEC07A2231ED8F27C3B7DB212A4E5F54CD5ED877 E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;..,|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_190632.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795064

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_190632.png	
Entropy (8bit):	7.944506064644382
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fRNy:ZSiGvxfK7ZMWSFpC6p8FE//frF/PA
MD5:	1286B3E1D9857F02198E3A565197A53A
SHA1:	82AB57535D4BC2C70ACD5D519D5DCBB5DF36C0C6
SHA-256:	C20BA1BF0D5E87D0062B1247998E81BAD0E2F5C2397748DE38E522F97EF7022D
SHA-512:	4049C153227D887F9DA6B3F09904AD8A0D88EB31DA2BDCE95D2E1B7CFE22DE507E01935154615B442851ACAF62C6D334D449FF035A647B14A457440F7486F60E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_191633.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795064
Entropy (8bit):	7.944506064644382
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fRNy:ZSiGvxfK7ZMWSFpC6p8FE//frF/PA
MD5:	1286B3E1D9857F02198E3A565197A53A
SHA1:	82AB57535D4BC2C70ACD5D519D5DCBB5DF36C0C6
SHA-256:	C20BA1BF0D5E87D0062B1247998E81BAD0E2F5C2397748DE38E522F97EF7022D
SHA-512:	4049C153227D887F9DA6B3F09904AD8A0D88EB31DA2BDCE95D2E1B7CFE22DE507E01935154615B442851ACAF62C6D334D449FF035A647B14A457440F7486F60E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_192634.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795129
Entropy (8bit):	7.943552777920506
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+F:ZSiGvxfK7ZMWSFpC6p8FE/Q9Ima9SeW
MD5:	ECAEA4C6C9CC78C158033127BE390B5C
SHA1:	41EECC4A1C94F22C32ECFA8036A691D9F076E314
SHA-256:	39AD908A3F20BD925E7EFA84299B39AEAEC13527F09652FA3050A681C55A16E1
SHA-512:	A4D0574B8844D22DD51B668426110409DF6246C330FCBCCEBB331DBE6517BAF52C79774A754B641807C417CDDD9336C02E4DB93E00D0EF7F375AB228AE132A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*..._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_193634.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795129
Entropy (8bit):	7.943552777920506
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+F:ZSiGvxfK7ZMWSFpC6p8FE/Q9Ima9SeW
MD5:	ECAEA4C6C9CC78C158033127BE390B5C
SHA1:	41EECC4A1C94F22C32ECFA8036A691D9F076E314
SHA-256:	39AD908A3F20BD925E7EFA84299B39AEAEC13527F09652FA3050A681C55A16E1

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_193634.png	
SHA-512:	A4D0574B8844D22DD51B668426110409DF6246C330FCBCCEBB331DBE6517BAF52C79774A754B641807C417CDDD9336C02E4DB93E00D0EF7F375AB228AE132A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_194637.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794782
Entropy (8bit):	7.944634143869951
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//funV:ZSiGvxfK7ZMWSFpC6p8FE//fuKNoA6
MD5:	7E4B1EB58538808E85E8EBAEA2152884
SHA1:	1E394754B9D59AEF73E32D45D5DBCEF83CB8D701
SHA-256:	D1F586998F5564C4C92DAA86F9861E9B26DB4AF1B523A633A53E7357953BE362
SHA-512:	38EAB3AE6A50EC71A6E5FF9F395E9CC7C259A89FD2DEF985CAA6AB0D01385E10993608F41C5F34C6C3004E85CDCF6FF7996A2AB0050834A6030DB52378FA245 0
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_195638.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794782
Entropy (8bit):	7.944634143869951
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//funV:ZSiGvxfK7ZMWSFpC6p8FE//fuKNoA6
MD5:	7E4B1EB58538808E85E8EBAEA2152884
SHA1:	1E394754B9D59AEF73E32D45D5DBCEF83CB8D701
SHA-256:	D1F586998F5564C4C92DAA86F9861E9B26DB4AF1B523A633A53E7357953BE362
SHA-512:	38EAB3AE6A50EC71A6E5FF9F395E9CC7C259A89FD2DEF985CAA6AB0D01385E10993608F41C5F34C6C3004E85CDCF6FF7996A2AB0050834A6030DB52378FA245 0
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_200638.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC 1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_200638.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_201639.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_202639.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_203640.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_203640.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_204640.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_205642.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795342
Entropy (8bit):	7.943548307920346
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/Quv+R:ZSiGvxfK7ZMWSFpC6p8FE/QTKjyPOC
MD5:	B950EB3A2A225A70D17FE269DE35A5DF
SHA1:	31215713F9CF099011C3AE1F7F94AB6D73BC3BFA
SHA-256:	EB98551D5D0C91DDF9049784C435205AEB5CA5750714E8A32DAC83CFFEC6B6D3
SHA-512:	62820C3B78D163E6D27FA589812291583491439 19B2D4DAAA1E98B9E04C690F6CDAFA520FE55CF486B71355D133E3E44F8533314797DF6F1F199F0299EE82F71
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_210644.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795064
Entropy (8bit):	7.944506064644382
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fRNy:ZSiGvxfK7ZMWSFpC6p8FE//frF/PA
MD5:	1286B3E1D9857F02198E3A565197A53A
SHA1:	82AB57535D4BC2C70ACD5D519D5DCBB5DF36C0C6
SHA-256:	C20BA1BF0D5E87D0062B1247998E81BAD0E2F5C2397748DE38E522F97EF7022D
SHA-512:	4049C153227D887F9DA6B3F09904AD8A0D88EB31DA2BDCE95D2E1B7CFE22DE507E01935154615B442851ACAF62C6D334D449FF035A647B14A457440F7486F60E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_211648.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	795064
Entropy (8bit):	7.944506064644382
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fRNy:ZSiGvxfK7ZMWSFpC6p8FE//frF/PA
MD5:	1286B3E1D9857F02198E3A565197A53A
SHA1:	82AB57535D4BC2C70ACD5D519D5DCBB5DF36C0C6
SHA-256:	C20BA1BF0D5E87D0062B1247998E81BAD0E2F5C2397748DE38E522F97EF7022D
SHA-512:	4049C153227D887F9DA6B3F09904AD8A0D88EB31DA2BDCE95D2E1B7CFE22DE507E01935154615B442851ACAF62C6D334D449FF035A647B14A457440F7486F60E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_212650.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	786044
Entropy (8bit):	7.944852902378266
Encrypted:	false
SSDEEP:	12288:n0zRFdVidv5vAu1EP2NFK1MFBJcxYinEtLa03cSp0WoYz+hNanc3en:0RFdKv5vFNFK1qeYY4GSdoSqNzi
MD5:	328647C12B0B258F7AF81E371936FF19
SHA1:	DC6A34C459EF718E922D914372AFEBE74B60207A
SHA-256:	75413346AF5A94FA30FB2E52E86003C0D328285C08B5625096BA26CBD09E4B7D
SHA-512:	A50810BE9DCEFB2CD9DCD35E10979A27BFFABDBCA6943BE0576D899105294AA33E5D2058F0A716161FDC40B029DC641A4D57FDF0F34D70DB35D6E2698CE6B 3A
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4Ey.....u7.....(..^p7.\1W..f1..cB.0F....#. n.... ..$.J.+..wpG....._=....9s.....LwUuuuw.S ..=.....Q..M..m7....;.7.dm..G..y.2.8.f.-#..j..V5.4.{.n..m.....\..Q1{...._.....[.....;....c.[.....[..v.8~..G,..mR....BWy~?..>f.~...}.....Y.M..i...c.K..TF*[.....7..v.g.:7\".=.n}MX.:....B.c<.. ..`..B.....~S.{/..^.XN...I\|...aQ.X...n..Q0..fCc.G4.....fp.m.1.)..6\....V...u.E...Z..v.k..x.+^111..s...R..'.....e...>.9H>t..._.n..I.....c.T.t.I...nH.s!m.Dm.[V.?.....c.O.9.k.j.<.Q..n. .2[...8.B.v...XZ...f..{...4.=9'{.x.SZ.h...@.Y.@...v|..3.c..D...LL.d.....$..4.Ge.e..T.|.'L.p..m....cZ.3.Q.M...I.....8Z..H.-.1.i...?...&&vj&...x..:.c./.7.e.o.....Fl.c.TV\..`m-..=t..,...b.....8 .cT..h....00.....`..@..D.Ohw.H4.uu.)6S.....c@.v.`:.p..c..`.....ANjO#..I....-x2..J$.~..-..b.....v.V.,...:..+.:].<.2.,_.c..uU..bm....`...t..... X.C..I!x-2...z..V.

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_213652.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC 1
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*.._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_214654.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_214654.png	
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!].h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_215655.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	794837
Entropy (8bit):	7.944700139262412
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE//fcBu:ZSiGvxfK7ZMWSFpC6p8FE//fcnbeWW
MD5:	DD498D1C92CDE90EE47FD8F35252E0DC
SHA1:	F4BE2048DF71EDB563275CF13716E66975FFC32C
SHA-256:	F1C1080E4C99742F10A77EDE8FA72A5BA38784A39751AD23D6F6C955B5A5452F
SHA-512:	6CCE7137A166435AC535E8072E349E791C9C675EF0659113E5827E179DE12AE6D7EDDF622827885B2F8601B091B30D4ED87058C13DBCCDDA742B71BDD8D6AC1
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!].h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_220657.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.,J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!].h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_221658.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_221658.png	
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',..J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_222659.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',..J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_223659.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',..J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_224700.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_224700.png	
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_225700.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_230701.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_231702.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_231702.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_232703.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_233705.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_234706.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_234706.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220104_235707.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	814951
Entropy (8bit):	7.943680227433188
Encrypted:	false
SSDEEP:	12288:1kdRqp9aXQ3wCaFaCdjVyXFh6wmHSs4Ze0HdJRn87hpoACTn4h:iXqp913wC7gyh69S1bRn87voFTk
MD5:	FBBFD6C60128020EB5A66086B16EB09A
SHA1:	86AAA2344F8D9F2FDE48DEE79AD797298BD3D911
SHA-256:	E9178C68915C2817022D88B7C41AA45856957728D6B1D440ACFB6F889109BA5B
SHA-512:	95020F8362C321DFE780576CE3FB11BBB5121187940978CB14D84FB29E005040E9C12D84B0210FE9AAD468FF41B91883253B12692348C95DA3A3045B921D0067
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...-Eu.....>..... ...UA.A...r..h..+.....8+.q.q..$~..gc..S..&*..Vu..V.....>.....>.....j.{{...!fi.C.v<., .t....l9"....X...u.|T...,.....[v.]....v.....}....Q....x...z..._.....;..s.}..n.X.y]..8...GYo.....q..c,dy.....*.Q..whX..E.Q..U)m.Q..n.w.....;..?.t..f.....M.G.7U.9.....oz..B.h.j.6;..b.&z./.YO...I. .*Q.....].....(.`N...]l.`YZ7a.S.iVl....h...2q....7..!`i..#N.....TC[OO6.:.....t..ck.3{p...Y.8G..-G....pb..'0..I..}.5...R4.'.....0.....5H9p....v.+.....mp.s2Sv..lB..y@...>..}n.Mk.....u...'.. ....8O...o..2.VB.8[...'P^.*;.&..{.[.<.opMv..Z.D.h!....'.....@=..O..>.P.\.fa*/.1.....[..4m.Q.B.$.Y..^....8..7..&.h.j.....a!.g..Q,.>.....}ZJ..i..kN{.%1.k.u.`..c...,.|...5...=.T....#...6_.Mg5 .v&.h.B.....`."...m..1<..[..9...P_.(o.....>9...8T.y2F..|k.....z...X...=.."P..0q.....@.../.&...b5. A.*M..).."o.$...?.h....r.#.....jG+.

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_000709.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_001710.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_001710.png	

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_002712.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_003716.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_004717.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_004717.png	
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_005718.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_010719.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@.....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_011721.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_011721.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_012722.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_013722.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_014723.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_014723.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',,...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_015723.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',,...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_020724.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',,...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_021724.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_021724.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',,...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_022725.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_023725.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',...@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_024726.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_024726.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_025727.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_030727.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j.....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_031728.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_031728.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_032728.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_033729.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4IU...m....(K7.....". .*.....0...,*..7;4....l....8." .,6....4(t.....'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.....e...'.`..n.s..bB:.+e..s.....9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[.....L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.....$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w.....P.....3.{...;...\|...=.ox...'.C..h..[u.'.P..I.N..n.....].f...1...I.t.vN.....M..c.k.....u..',.J...3.0.J.....EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....]..M_...c.O.%..j.<.Q.....2..a..m.....u...4.=...L..D8....@...@.?A.@....\.). ..J.....j....`.!.....*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._..n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_034729.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	801665
Entropy (8bit):	7.943053037734203
Encrypted:	false
SSDEEP:	24576:0RFdKv5vFNFK1qeYY4GSBfiCloXpRMu5X:4FOdNE8eY9DqClipCu5X
MD5:	859130BB4E8B241BAB2A8D894D083558
SHA1:	9FC669AACE7616EA953E42C31F7B2AEA9FBB4BEA
SHA-256:	D41976C978798B58BB1B4E3C23F7E374005D571751F72EDF21FE83169DA990D1
SHA-512:	C5D77A1460DC9908E1634632F06CB7E0B93D718A18967BCA6AEE329CB63E020324BC8B1C1CF07D1384A15EDA69BF14C1D9825D39E3D28436CFA1111800FB481
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...4Ey.....u7.....(..^p7.\1W..f1..cB.0F....#. n.... ..$.J.+..wpG....._=....9s.....LwUuuuw.S ..=.....Q..M..m7....;.7.dm..G..y.2.8.f.-#..j..V5.4.{.n..m.....\..Q1{...._.....[.....;....c.[.....[..v.8~..G,..mR....BWy~?..>f.~...}.....Y.M..i...c.K..TF*[.....7..v.g.:7\".=.n}MX.:.....B.c<.. ..`..B.....~S.{/..^.XN...I|...aQ.X...n..Q0..fCc.G4.....fp.m.1.)..6\....V...u.E...Z..v.k..x.+^111..s...R..'.....e...>.9H>t..._.n..I.....c.T.t.I...nH.s!m.Dm.[V.?.....c.O.9.k.j.<.Q..n. .2[...8.B.v...XZ...f..{...4.=9'{.x.SZ.h...@.Y.@...v|..3.c..D...LL.d.....$..4.Ge.e..T..|.'L.p..m....cZ.3.Q.M...I....8Z..H.-.1.i...?...&&vj&...x...:.c./.7.e.o.....Fl.c.TV\..`m-..=t..,..b.....8 .cT..h....00.....`..@..D.Ohw.H4.uu.)6S.....c@.v.`:.p..c..`.....ANjO#..I....-x2..J$.~..-..b.....v.V.,...:..+.:].<.2.,_.c..uU..bm....`...t.... X.C..I!x-2...z..V.

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_034729.png

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_035730.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.................C....sRGB.........gAMA......a.....pHYs.........o.d....IDATx^...4IU...m....(K7......". .*......0...,*..7;4....l....8." .,6....4(t......'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.......e...'.`..n.s..bB:.+e..s.........9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[......L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.......$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w......P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n......].f...1...I.t.vN......M..c.k.....u..',.J...3.0.J.......EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q......2..a..m.............u...4.=...L..D8....@...@.?A.@.....\.). ..J.......j.....`.!.......*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

C:\Users\user\AppData\Roaming\Screenshots\time_20220105_040730.png	
Process:	C:\Users\user\AppData\Local\Temp\rem.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	810227
Entropy (8bit):	7.944312483525065
Encrypted:	false
SSDEEP:	12288:ZrtgEzGvXLNfiPB1rtH/M4tx7eYP0MHlc/FPxU/ARwEdSLmOoWrN/C8oWE/tV8Nq:ZSiGvxfK7ZMWSFpC6p8FE/tV8zmBcM
MD5:	776A0435F0E79D7C7318403B9D7AF336
SHA1:	8B2B8962D3963E53B4771C7AF4F26DDBF3518CD3
SHA-256:	907C81063465F5B91D9599AAC6327F85814190EED73F5815B0BDFC2A6D35412A
SHA-512:	A6F76BFDBCFC19F676297E4DAF4900F8211F8EEB07BE33F3D2874CCA975608E35EB3191EBC33D9FCAD822A0FC2BC3FA0C82B8D32CEDD4722079343341E3E16FD
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.................C....sRGB.........gAMA......a.....pHYs.........o.d....IDATx^...4IU...m....(K7......". .*......0...,*..7;4....l....8." .,6....4(t......'..oDFde..}u...TU,'....{3.vv.y.n .Z7.9.{..cn.....|...k.@..7k..7.9t.......e...'.`..n.s..bB:.+e..s.........9t...~...}).|..s.Z...Z\3.n..f..s..~.\G.[......L.d.s.....kU...6..o1.w..sMi.2.....!...d[..s..k.7..^....k\..HyRn?',6.g.[)x.......$t ,dH.3.G.}..{/L./..S..g..."f}X..W.q..w......P.....3.{....;...|...=.ox...'.C..h..[u.'.P..I.N..n......].f...1...I.t.vN......M..c.k.....u..',.J...3.0.J.......EU.5u...R.=.1.+...U....5<..M=..c.x.`./Cl,.....].. M_...c.O.%..j.<.Q......2..a..m.............u...4.=...L..D8....@...@.?A.@.....\.). ..J.......j.....`.!.......*._.....2`.L"..c..L<..[...V.\..Gq$..L,-...3....l...&.....g#./d-....cDg.z...._.n..bH?..... ..Z.p.p..k....4...Sb...Z?.}T.;.....j..g[.m..{..e...a..p....z...?!]..h3*-.9.S..dQ...Ag..iS',....@.1n...O..D....A..d.@...`b.JD:.l.[0....k..8.i9..c..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.983843341962055
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SW0P9o9ksjpBsnr.exe
File size:	2203648
MD5:	27f2a9688ec34fc8aa3b0fee4757dd71

General

SHA1:	9464f6bea3222c5598ecd9d29a8bc68c0998f926
SHA256:	5733ad0577f5b8fc7e939b1daff3ff98b339bb47542a138b659e47b9001fbbd2
SHA512:	c53a2a9efa08002acc8f4304bb7eff7b9e4ebd9e9dc0c5d2c73ad6798c59f2b851bce30c72389218c05ca5c8f562df38e1199950115f69e35cb6822462419544
SSDEEP:	49152:Fk027OjSrCkg7gybKAOAM0hfucdaX2MEGfxDN+JAAPP6VvuHR:F/02OMxVOApAcdiEGfBN0Au6h
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..a.....0...!.....N.!.. ...!...@.. .....".....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x61b54e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61CBBF48 [Wed Dec 29 01:52:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x219554	0x219600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x21c000	0x600	0x600	False	0.434895833333	data	4.21140615582	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x21e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, 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
01/04/22-15:06:23.823422	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	104.16.155.36	192.168.2.5
01/04/22-15:06:24.046804	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	104.16.155.36	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 4, 2022 15:06:22.666641951 CET	192.168.2.5	8.8.8.8	0x8478	Standard query (0)	9.96.11.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 4, 2022 15:06:23.713320017 CET	192.168.2.5	8.8.8.8	0x5de0	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:46.030277967 CET	192.168.2.5	8.8.8.8	0x3434	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:48.689799070 CET	192.168.2.5	8.8.8.8	0x12b0	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:50.589838982 CET	192.168.2.5	8.8.8.8	0xbed8	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:54.605858088 CET	192.168.2.5	8.8.8.8	0x7ac7	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:58.519088984 CET	192.168.2.5	8.8.8.8	0xa5a2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:02.679861069 CET	192.168.2.5	8.8.8.8	0x5a38	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:06.995929003 CET	192.168.2.5	8.8.8.8	0x895c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:11.955128908 CET	192.168.2.5	8.8.8.8	0x2ad2	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:17.009006977 CET	192.168.2.5	8.8.8.8	0xc09f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:22.315131903 CET	192.168.2.5	8.8.8.8	0x8865	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:28.313379049 CET	192.168.2.5	8.8.8.8	0xccb0	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:34.146763086 CET	192.168.2.5	8.8.8.8	0x771c	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:40.216717005 CET	192.168.2.5	8.8.8.8	0xbd9b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:47.117548943 CET	192.168.2.5	8.8.8.8	0x3256	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:50.891854048 CET	192.168.2.5	8.8.8.8	0x28fd	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 15:06:22.685647011 CET	8.8.8.8	192.168.2.5	0x8478	Name error (3)	9.96.11.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 4, 2022 15:06:23.731823921 CET	8.8.8.8	192.168.2.5	0x5de0	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:23.731823921 CET	8.8.8.8	192.168.2.5	0x5de0	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:46.050786018 CET	8.8.8.8	192.168.2.5	0x3434	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 4, 2022 15:06:48.709620953 CET	8.8.8.8	192.168.2.5	0x12b0	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:50.610759020 CET	8.8.8.8	192.168.2.5	0xbed8	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:54.624644041 CET	8.8.8.8	192.168.2.5	0x7ac7	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:06:58.539190054 CET	8.8.8.8	192.168.2.5	0xa5a2	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:02.697153091 CET	8.8.8.8	192.168.2.5	0x5a38	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:07.015086889 CET	8.8.8.8	192.168.2.5	0x895c	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:11.978346109 CET	8.8.8.8	192.168.2.5	0x2ad2	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:17.029227972 CET	8.8.8.8	192.168.2.5	0xc09f	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:22.335664034 CET	8.8.8.8	192.168.2.5	0x8865	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:28.331489086 CET	8.8.8.8	192.168.2.5	0xccb0	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:34.165414095 CET	8.8.8.8	192.168.2.5	0x771c	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:40.233660936 CET	8.8.8.8	192.168.2.5	0xbd9b	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:47.136590958 CET	8.8.8.8	192.168.2.5	0x3256	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Jan 4, 2022 15:07:50.912226915 CET	8.8.8.8	192.168.2.5	0x28fd	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49765	104.16.155.36	80	

Timestamp	kBytes transferred	Direction	Data
Jan 4, 2022 15:06:23.793555021 CET	1145	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jan 4, 2022 15:06:23.823421955 CET	1146	IN	HTTP/1.1 403 Forbidden Date: Tue, 04 Jan 2022 14:06:23 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=9.gsBxN_TlFUSbreDLPbWL6FYpa.GN4p00zBzeoSM3A-1641305183-0-AeUdY+n5LN7US DwNfmj5TSRNGaWztIYvAklLwEwNucw9pUZwZ2l2ZbjFQzDfD62xzB8G6jLZy8vOobUN/MZShNg=; path=/; expires=Tue, 04-Jan-22 14:36:23 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6c8506f6cf196997-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

Timestamp	kBytes transferred	Direction	Data
Jan 4, 2022 15:06:24.046803951 CET	1147	IN	HTTP/1.1 403 Forbidden Date: Tue, 04 Jan 2022 14:06:23 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=9.gsBxN_TlFUSbreDLPbWL6FYpa.GN4p00zBzeoSM3A-1641305183-0-AeUdY+n5LN7US DwNfmj5TSRNGaWztIYvAklLwEwNucw9pUZwZ2l2ZbjFQzDfD62xzB8G6jLZy8vOobUN/MZShNg=; path=/; expires=Tue, 04-Jan-22 14:36:23 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6c8506f6cf196997-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
Jan 4, 2022 15:06:46.421114922 CET	587	49792	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:06:46.421591997 CET	49792	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:06:46.611622095 CET	587	49792	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:06:46.611896992 CET	49792	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:06:46.810611010 CET	587	49792	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:06:49.138483047 CET	587	49795	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:06:51.386814117 CET	587	49797	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:06:51.387156963 CET	49797	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:06:51.575973034 CET	587	49797	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:06:55.005717039 CET	587	49801	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:06:55.006125927 CET	49801	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:06:55.179908991 CET	587	49801	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:06:55.180218935 CET	49801	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:06:55.359390974 CET	587	49801	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:06:58.884766102 CET	587	49812	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:06:58.884994984 CET	49812	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:06:59.061115026 CET	587	49812	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:06:59.061346054 CET	49812	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:06:59.247302055 CET	587	49812	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:03.044284105 CET	587	49815	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:03.047522068 CET	49815	587	192.168.2.5	66.29.159.53	EHLO 745481

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 4, 2022 15:07:03.229331970 CET	587	49815	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:03.231827974 CET	49815	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:03.412834883 CET	587	49815	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:07.378546000 CET	587	49820	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:07.378879070 CET	49820	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:07.556359053 CET	587	49820	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:07.556588888 CET	49820	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:07.727467060 CET	587	49820	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:12.349395037 CET	587	49828	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:12.349598885 CET	49828	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:12.520612955 CET	587	49828	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:12.520833015 CET	49828	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:12.686464071 CET	587	49828	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:17.387933016 CET	587	49833	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:17.388262033 CET	49833	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:17.564378023 CET	587	49833	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:17.564765930 CET	49833	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:17.746862888 CET	587	49833	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:22.703813076 CET	587	49841	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:22.704210997 CET	49841	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:22.880002022 CET	587	49841	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:22.880523920 CET	49841	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:23.047652006 CET	587	49841	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:28.688891888 CET	587	49846	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:28.689121962 CET	49846	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:28.873761892 CET	587	49846	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:28.874133110 CET	49846	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:29.063883066 CET	587	49846	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:34.570219994 CET	587	49850	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node

Copyright Joe Security LLC 2022

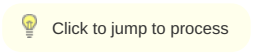
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 4, 2022 15:07:34.570785999 CET	49850	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:34.764210939 CET	587	49850	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:34.764679909 CET	49850	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:34.955817938 CET	587	49850	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:40.621457100 CET	587	49856	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:40.621748924 CET	49856	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:40.794528961 CET	587	49856	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:40.795001984 CET	49856	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:40.968621969 CET	587	49856	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:47.483863115 CET	587	49861	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:47.484101057 CET	49861	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:47.664139032 CET	587	49861	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:47.665640116 CET	49861	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:47.845174074 CET	587	49861	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:48.294898987 CET	587	49862	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:48.295043945 CET	49862	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:48.484863997 CET	587	49862	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:48.485013962 CET	49862	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:48.672544003 CET	587	49862	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:50.919059038 CET	587	49864	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:50.919236898 CET	49864	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:50.956199884 CET	587	49865	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:50.956459999 CET	49865	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:51.100640059 CET	587	49864	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:51.100797892 CET	49864	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:51.133240938 CET	587	49865	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:51.133446932 CET	49865	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:51.277748108 CET	587	49864	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:51.308254957 CET	587	49865	66.29.159.53	192.168.2.5	220 Ready to start TLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 4, 2022 15:07:51.311764956 CET	587	49866	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:51.312067032 CET	49866	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:51.500338078 CET	587	49866	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:51.500576019 CET	49866	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:51.691961050 CET	587	49866	66.29.159.53	192.168.2.5	220 Ready to start TLS
Jan 4, 2022 15:07:58.125185013 CET	587	49871	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
Jan 4, 2022 15:07:58.125361919 CET	49871	587	192.168.2.5	66.29.159.53	EHLO 745481
Jan 4, 2022 15:07:58.320297003 CET	587	49871	66.29.159.53	192.168.2.5	250-mta-10.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jan 4, 2022 15:07:58.320461035 CET	49871	587	192.168.2.5	66.29.159.53	STARTTLS
Jan 4, 2022 15:07:58.519264936 CET	587	49871	66.29.159.53	192.168.2.5	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SW0P9o9ksjpBsnr.exe PID: 5468 Parent PID: 6036

General

Start time:	15:05:40
Start date:	04/01/2022
Path:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe"
Imagebase:	0x800000
File size:	2203648 bytes
MD5 hash:	27F2A9688EC34FC8AA3B0FEE4757DD71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.287902028.0000000002CDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Florian Roth • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.289270631.0000000003C99000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: BackgroundTransferHost.exe PID: 4928 Parent PID: 792

General

Start time:	15:05:45
Start date:	04/01/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff612ab0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Copyright Joe Security LLC 2022

Analysis Process: SW0P9o9ksjpBsnr.exe PID: 4928 Parent PID: 5468

General

Start time:	15:05:52
Start date:	04/01/2022
Path:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SW0P9o9ksjpBsnr.exe
Imagebase:	0xf60000
File size:	2203648 bytes
MD5 hash:	27F2A9688EC34FC8AA3B0FEE4757DD71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000003.291798891.0000000004593000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.291798891.0000000004593000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.291798891.0000000004593000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.291798891.0000000004593000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.307369542.00000000045AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.315881747.0000000003ECD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000003.315881747.0000000003ECD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.330768411.0000000004525000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000000.283855450.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.309595356.0000000003ECE000.00000004.00000001.sdmp,

Author: Joe Security
- Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000003.309595356.0000000003ECE000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.329717962.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.313272509.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.286683979.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.315166060.0000000003ECD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000000.282034651.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.286824707.0000000003ECC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.328524290.00000000044B8000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.325603575.0000000004481000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author:

	Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.331133641.0000000000403000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Analysis Process: bin.exe PID: 6480 Parent PID: 4928

General

Start time:	15:05:59
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\bin.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bin.exe" 0
Imagebase:	0x880000
File size:	115712 bytes
MD5 hash:	805FBB84293E86F25B566A5B2C2815D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000003.295733640.00000000010D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000003.295733640.00000000010D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000003.295896513.00000000010CE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000003.295896513.00000000010CE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000000.291633552.0000000000894000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000000.291633552.0000000000894000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000000.291260710.0000000000894000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000000.291260710.0000000000894000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000003.295581021.00000000010D3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000003.295581021.00000000010D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000003.295581021.00000000010D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000003.295581021.00000000010D3000.00000004.00000001.sdmp, Author:

Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000000.291654350.00000000009CF000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000000.291654350.00000000009CF000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000002.525512056.00000000009CF000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000002.525512056.00000000009CF000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.525142353.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.525142353.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000000.290415827.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000000.290415827.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000003.295601289.00000000010E4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000003.295601289.00000000010E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000003.295697323.00000000010E4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000003.295697323.00000000010E4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000002.533158869.0000000003085000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000002.533158869.0000000003085000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.533158869.0000000003085000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.533158869.0000000003085000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000000.290450731.00000000009CF000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000000.290450731.00000000009CF000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000000.290858967.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000000.290858967.0000000000894000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000000.291282105.00000000009CF000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000000.291282105.00000000009CF000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000B.00000000.290889845.00000000009CF000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000B.00000000.290889845.00000000009CF000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source:

	C:\Users\user\AppData\Local\Temp\bin.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, Metadefender, Browse • Detection: 89%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: warz.exe PID: 6544 Parent PID: 4928

General

Start time:	15:06:00
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\warz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\warz.exe" 0
Imagebase:	0x1020000
File size:	115712 bytes
MD5 hash:	1D90A7DA17807F64F1699E5EA2091A36
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000000.294569462.0000000001034000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000000.294569462.0000000001034000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000002.311194083.000000000116F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000002.311194083.000000000116F000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000003.299504412.0000000000DA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000003.299504412.0000000000DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000000.293488925.0000000001034000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000000.293488925.0000000001034000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000002.312181908.0000000002FD7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000002.312181908.0000000002FD7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.312181908.0000000002FD7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000002.312181908.0000000002FD7000.00000004.00000001.sdmp, Author: Joe Security

- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.300135911.0000000000D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.300135911.0000000000D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000003.305332768.0000000000DA2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000003.305332768.0000000000DA2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.305332768.0000000000DA2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.305332768.0000000000DA2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000003.299610781.0000000000DA2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000003.299610781.0000000000DA2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000000.294592566.000000000116F000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000000.294592566.000000000116F000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.310994580.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000002.310994580.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000000.294916604.000000000116F000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000000.294916604.000000000116F000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.300261604.0000000000D8C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.300261604.0000000000D8C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000003.299968878.0000000000DA2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000003.299968878.0000000000DA2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.299137914.0000000000D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.299137914.0000000000D91000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000000.293514502.000000000116F000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000000.293514502.000000000116F000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000000.294897016.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000000.294897016.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000000.293955227.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000000.293955227.0000000001034000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000000.294003890.000000000116F000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000000.294003890.000000000116F000.00000002.00020000.sdmp, Author: Joe Security

	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\warz.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, Metadefender, Browse • 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

Key Value Modified

Analysis Process: rem.exe PID: 6564 Parent PID: 4928

General

Start time:	15:06:02
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\rem.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\rem.exe" 0
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	9E764165FBA9E86937643D84A2F4E063
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000000.296555205.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000000.297395374.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000000.298936574.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000000.298035428.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\rem.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\rem.exe, Author: unknown

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 50%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 6572 Parent PID: 6480

General

Start time:	15:06:02
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 6580 Parent PID: 6480

General

Start time:	15:06:02
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000002.528440483.0000000003290000.00000004.00000001.sdmp, Author: unknown
Reputation:	high

Analysis Process: conhost.exe PID: 6588 Parent PID: 6572

General

Start time:	15:06:02
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: conhost.exe PID: 6596 Parent PID: 6580

General

Start time:	15:06:02
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: powershell.exe PID: 6764 Parent PID: 6544

General

Start time:	15:06:04
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: hawkstartup.exe PID: 6776 Parent PID: 4928

General

Start time:	15:06:04
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\hawkstartup.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\hawkstartup.exe" 0
Imagebase:	0x4d0000
File size:	532992 bytes
MD5 hash:	AEAF1943FB037B6529873D7CC47CE137
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: 00000013.00000000.303483748.00000000004D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.303483748.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000000.303483748.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000000.303483748.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000000.303483748.00000000004D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000013.00000000.302582186.00000000004D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.302582186.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000000.302582186.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000000.302582186.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000000.302582186.00000000004D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000013.00000000.304045039.00000000004D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.304045039.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000000.304045039.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000000.304045039.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000000.304045039.00000000004D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000013.00000002.331424060.00000000004D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source:

	00000013.00000002.331424060.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.331424060.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.331424060.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000002.331424060.00000000004D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000013.00000000.305406305.00000000004D2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000000.305406305.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000000.305406305.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000000.305406305.00000000004D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000013.00000000.305406305.00000000004D2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.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\hawkstartup.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Local\Temp\hawkstartup.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: conhost.exe PID: 6808 Parent PID: 6764

General

Start time:	15:06:05
Start date:	04/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: images.exe PID: 6824 Parent PID: 6544

General

Start time:	15:06:05
Start date:	04/01/2022
Path:	C:\ProgramData\images.exe

Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x330000
File size:	115712 bytes
MD5 hash:	1D90A7DA17807F64F1699E5EA2091A36
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.524091426.0000000000344000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000002.524091426.0000000000344000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000002.533537328.00000000036E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000002.533537328.00000000036E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.533537328.00000000036E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000002.533537328.00000000036E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000002.524271296.000000000047F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000002.524271296.000000000047F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000000.304556285.0000000000344000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000000.304556285.0000000000344000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000003.315134280.00000000014B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000003.315134280.00000000014B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000003.315040551.00000000014B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000003.315040551.00000000014B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000000.304645862.000000000047F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000000.304645862.000000000047F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000003.315866343.000000000149C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000003.315866343.000000000149C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000003.314784536.00000000014A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000003.314784536.00000000014A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000016.00000003.315520254.00000000014B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000016.00000003.315520254.00000000014B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\ProgramData\images.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\ProgramData\images.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\ProgramData\images.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, Metadefender, Browse • Detection: 89%, ReversingLabs
Reputation:	low

Analysis Process: ori4.0dec23sta.exe PID: 6988 Parent PID: 4928

General

Start time:	15:06:09
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe" 0
Imagebase:	0x8c0000
File size:	221184 bytes
MD5 hash:	F41809BC71EEB2C3B1676309139216A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.312592775.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.312592775.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.535498447.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.535498447.0000000002D41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.313041784.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.313041784.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.523672410.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.523672410.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.311207048.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.311207048.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.311917188.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.311917188.00000000008C2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori4.0dec23sta.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 51%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 7092 Parent PID: 6824

General

Start time:	15:06:11
Start date:	04/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x2b0000
File size:	430592 bytes

MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: ori2.0dec23sta.exe PID: 7112 Parent PID: 4928

General

Start time:	15:06:11
Start date:	04/01/2022
Path:	C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe" 0
Imagebase:	0xd0000
File size:	220672 bytes
MD5 hash:	421138225D5DEE81805C5E5072898504
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000003.364545271.00000000056D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000003.364545271.00000000056D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.322486737.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.322486737.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.324705647.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.324705647.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.523856737.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000002.523856737.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.317498484.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.317498484.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.317967503.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.317967503.00000000000D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.534940156.0000000002721000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.534940156.0000000002721000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\ori2.0dec23sta.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, ReversingLabs

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022