ID: 715156
Sample Name: pebbles.dat.dll
Cookbook: default.jbs
Time: 17:38:53
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

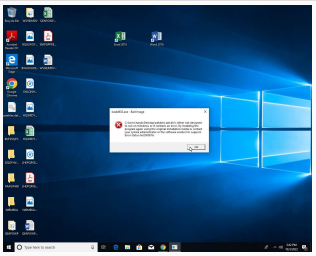
Windows Analysis Report

pebbles.dat.dll

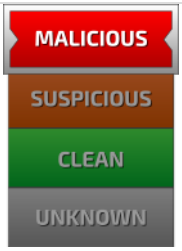
Overview

General Information

Sample Name:	pebbles.dat.dll
Analysis ID:	715156
MD5:	d89521adaf6418..
SHA1:	38cac8495ef43e...
SHA256:	1965dc57456d4f..
Tags:	dll
Infos:	



Detection



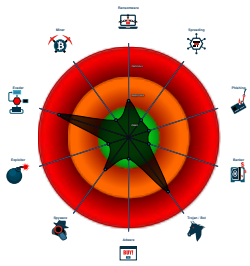
Qbot

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Qbot
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: Execute DLL with s...
- Maps a DLL or memory area into an...
- Overwrites code with unconditional j...
- Writes to foreign memory regions
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...
- Allocates memory in foreign process...
- Uses 32bit PE files
- Queries the volume information (nam...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5328 cmdline: loaddll32.exe "C:\Users\user\Desktop\pebbles.dat.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5900 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5792 cmdline: rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - wermgr.exe (PID: 4884 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - regsvr32.exe (PID: 5696 cmdline: regsvr32.exe /s C:\Users\user\Desktop\pebbles.dat.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - wermgr.exe (PID: 3472 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
    - audiodg.exe (PID: 3472 cmdline: C:\Windows\system32\AUDIODG.EXE 0x2ac MD5: 0B245353F92DF527AA7613BA2C0DA023)
  - rundll32.exe (PID: 5784 cmdline: rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 612 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 5360 cmdline: rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5580 cmdline: rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,bewailable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x10f4f:$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00

Source	Rule	Description	Author	Strings
00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Qbot_3074a8d4	unknown	unknown	• 0x1ca14:$a4: %u;%u;%u; • 0x1cf50:$a5: %u.%u.%u.%u.%u.%u.%04x • 0x1cdd8:$a6: %u&%s&%u • 0x8cc6:$get_string1: 33 D2 8B C6 6A 5A 5F F7 F7 8B 7D 08 8A 04 3A 8B 55 F8 8B 7D 10 3A 04 16 • 0x9004:$set_key: 8D 87 00 04 00 00 50 56 E8 BF 15 00 00 59 8B D0 8B CE E8 • 0x3330:$do_computer_use_russian_like_keyboard: B9 F F 03 00 00 66 23 C1 33 C9 0F B7 F8 66 3B 7C 4D • 0x2d87:$execute_each_tasks: 8B 44 0E 0C 85 C0 74 04 FF D0 EB 12 6A 00 6A 00 6A 00 FF 74 0E 08 E8 F5 EF F F FF 83 C4 10 • 0xc8ee:$generate_random_alpha_num_string: 57 E8 DC DC FF FF 48 50 8D 85 30 F6 FF FF 6A 00 50 E8 D1 6D 0 0 00 8B 4D F8 83 C4 10 8A 04 38 88 04 0E 46 83 FE 0C
00000003.00000002.269120079.0000000000990000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000003.00000002.269120079.0000000000990000.00000040.00000800.00020000.00000000.sdmp	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x10f4f:$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.wermgr.exe.970000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
9.2.wermgr.exe.970000.0.raw.unpack	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x10f4f:$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00
9.2.wermgr.exe.970000.0.raw.unpack	Windows_Trojan_Qbot_3074a8d4	unknown	unknown	• 0x1ca14:$a4: %u;%u;%u; • 0x1cf50:$a5: %u.%u.%u.%u.%u.%u.%04x • 0x1cdd8:$a6: %u&%s&%u • 0x8cc6:$get_string1: 33 D2 8B C6 6A 5A 5F F7 F7 8B 7D 08 8A 04 3A 8B 55 F8 8B 7D 10 3A 04 16 • 0x9004:$set_key: 8D 87 00 04 00 00 50 56 E8 BF 15 00 00 59 8B D0 8B CE E8 • 0x3330:$do_computer_use_russian_like_keyboard: B9 F F 03 00 00 66 23 C1 33 C9 0F B7 F8 66 3B 7C 4D • 0x2d87:$execute_each_tasks: 8B 44 0E 0C 85 C0 74 04 FF D0 EB 12 6A 00 6A 00 6A 00 FF 74 0E 08 E8 F5 EF F F FF 83 C4 10 • 0xc8ee:$generate_random_alpha_num_string: 57 E8 DC DC FF FF 48 50 8D 85 30 F6 FF FF 6A 00 50 E8 D1 6D 0 0 00 8B 4D F8 83 C4 10 8A 04 38 88 04 0E 46 83 FE 0C
3.2.regsvr32.exe.990000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
3.2.regsvr32.exe.990000.0.raw.unpack	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x10f4f:$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00
Click to see the 61 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Stealing of Sensitive Information

Yara detected Qbot

Remote Access Functionality

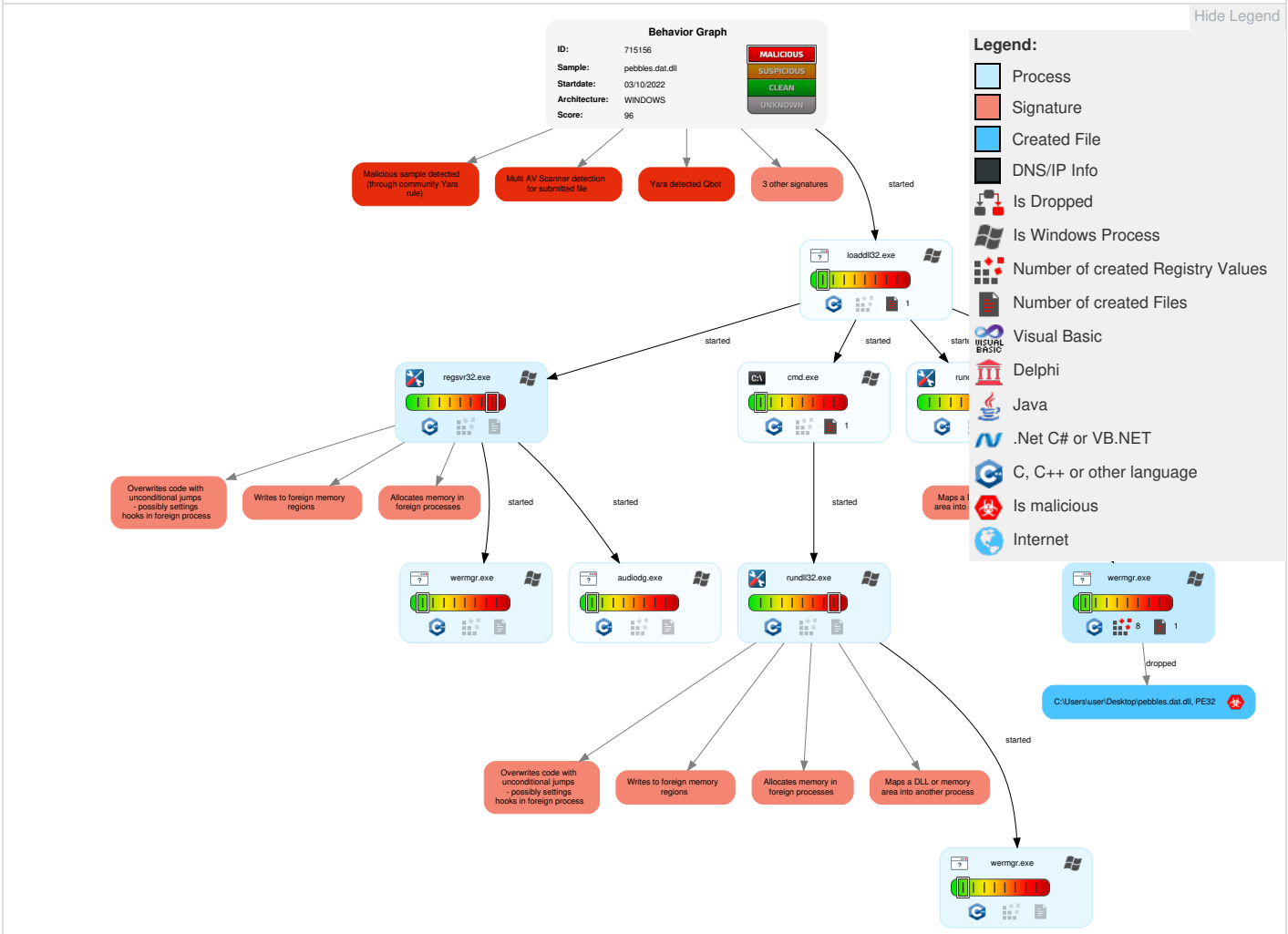
Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 DLL Side-Loading	3 1 1 Process Injection	1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Regsvr32	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

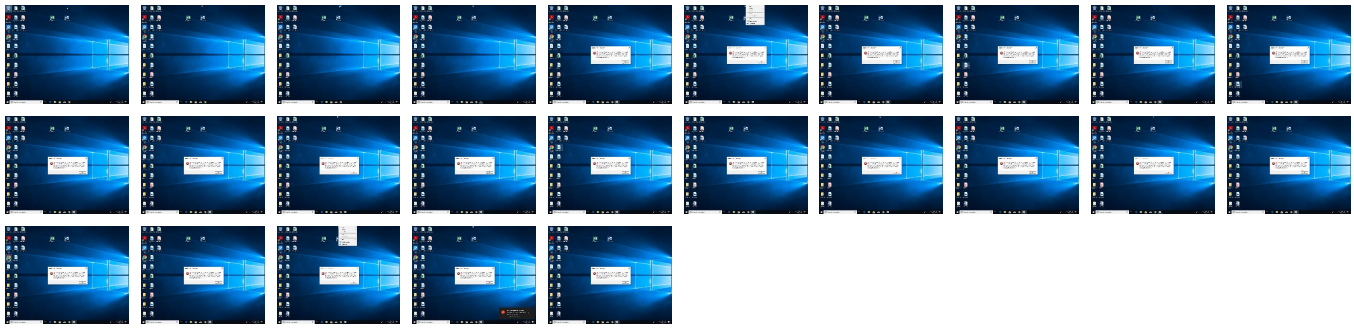
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
pebbles.dat.dll	17%	ReversingLabs		
pebbles.dat.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.wermgr.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
8.0.wermgr.exe.12a0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
3.2.regsvr32.exe.990000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
4.2.rundll32.exe.4450000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
9.0.wermgr.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.wermgr.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
5.2.rundll32.exe.2ee0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
7.0.wermgr.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715156
Start date and time:	2022-10-03 17:38:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pebbles.dat.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	38
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:	mal96.troj.evad.winDLL@21/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.3% (good quality ratio 24%) • Quality average: 77.1% • Quality standard deviation: 26.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\pebbles.dat.dll

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.667100449217363
Encrypted:	false
SSDEEP:	96:UORfeVXzt2Dk1dyqIF9JhsLwAOhf2ZW2wIPD:UORAjMkXIKPD
MD5:	21928784DA52AB71A60AF59EFA95CDAD
SHA1:	4FF8ECD9B0370614EA0C3D8583A51DF9D2481844
SHA-256:	285861283C9DC3F2D892B3CC186AD64CF17217D394B227A70B6C657C39D6568B
SHA-512:	CD79DFD111B8E1E8A3EB2F7E57DFB71D76AF677D6696564C15413391D7734F0C4A10D3987A3D4D9739C082C0710BC5B8566A4D4AB295EA501B5D909D0294C3 8
Malicious:	**true**

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.....~[..~[..~[..}Z..~[..{Z..~[..zZ..~[I.zZ..~[I.}Z..~[I.{ZX.~[...Z..~[...[o.~[..wZ..~[..~Z..~[..[..~[...[..~[..|Z..~[Rich..~[.....PE..L.....:c.....!.....~.....0.....@.....p.....A..P..... ...6.....p.....0...@.....@.....data....a.....b..... ....reloc6s.....f..... ..`CODE.....0.....idata..0....@..... .....@..@.hata....5...P...6.....@..@DATA....T.....J.....@..@.rsrc.....L.....@..@.reloc...6.....8...N.....@..B..... .....

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.9607693404023925
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	pebbles.dat.dll
File size:	493056
MD5:	d89521adaf6418e6ebe43b1a1a9d2af9
SHA1:	38cac8495ef43e51cdac1cb5e85d10137b365bee
SHA256:	1965dc57456d4fc01b6ce0f242d80776fe08a16354e6177255cba618348355ac
SHA512:	703db1e11372070dbbabc8a96c8600f079273e4dfad4e5437a5fd4b046187cf9f24b47ad68fadaf3bcf7fb1dcad8ecf98edd299281938eb144c4c6c29d68461f
SSDEEP:	12288:Y2X+B4HKFVxT5jXAcOf35HI9H5RGqdIhr54f:L5EVl5DC4HDbd
TLSH:	DBA48D0AB612C430D66910B12876BBE047ACBD325E751EDF73805F778A641F77A29F22
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.....~[..~[..~[..}Z..~[..{Z..~[..zZ..~[I.zZ..~[I.}Z..~[I.{ZX.~[...Z..~[...[o.~[..wZ..~[..~Z..~[...[..~[...[..~[..|Z..~[Rich..~

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100382d9
Entrypoint Section:	.data
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x633AE6FF [Mon Oct 3 13:43:27 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	8877a7b766af3aace7fcad8462a174cc

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FD97CC082C7h
call 00007FD97CC087E4h

Instruction
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FD97CC08173h
add esp, 0Ch
pop ebp
retn 000Ch
cmp ecx, dword ptr [10001D84h]
jne 00007FD97CC082C3h
ret
jmp 00007FD97CC088CDh
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [10001D84h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [10001D84h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 0Fh
add eax, ecx
sbb ecx, ecx
or eax, ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x57010	0x10f	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74188	0x50	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7a000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7b000	0x36b4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x311c0	0x70	.data
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x31230	0x40	.data
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x74000	0x184	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x1000	0x5611f	0x56200	False	0.6558956594702468	data	7.0153365923230595	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc6s	0x58000	0x1a0f9	0x1a200	False	0.3239383971291866	COM executable for DOS	6.066972398111804	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
CODE	0x73000	0x200	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x74000	0xa30	0xc00	False	0.404296875	data	4.897788340416598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hata	0x75000	0x35e7	0x3600	False	0.7127459490740741	data	5.561450278641814	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
DATA	0x79000	0x54	0x200	False	0.162109375	data	1.2433795844140498	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x1e0	0x200	False	0.53125	data	4.724728911998389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7b000	0x36b4	0x3800	False	0.7310267857142857	data	6.633507194727193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x7a060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	Sleep, DebugBreak, GetCurrentProcess, lstrlenA, GetCurrentThreadId, lstrcmpA, VirtualAlloc, GetVersion, GetCommandLineA, GetFileAttributesA, GetCurrentThread, GetCurrentProcessId, GetModuleHandleW, lstrcmpiA, CreateFileW, CloseHandle, GetModuleHandleA, GetConsoleMode, GetConsoleOutputCP, WriteFile, FlushFileBuffers, HeapSize, SetStdHandle, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, MultiByteToWideChar, LCMapStringEx, GetStringTypeW, GetCPInfo, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, RaiseException, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapAlloc, HeapFree, GetStdHandle, GetFileType, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, MoveFileExW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, SetFilePointerEx, WriteConsoleW
ADVAPI32.dll	CryptCreateHash, CryptHashData, CryptDestroyHash, CryptGetHashParam, CryptReleaseContext, CryptAcquireContextA
SHLWAPI.dll	PathFindExtensionA, PathFindOnPathA, PathFileExistsA, PathFindSuffixArrayA, StrToIntA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x1006eb00
DllUnregisterServer	2	0x1006f6f0
bewailable	3	0x10058e00
courtlet	4	0x10063590
noncensored	5	0x10067e60
rhizocarpean	6	0x100605f0
stine	7	0x10069040
strigiles	8	0x1005de90
targetlike	9	0x1006b820
trimethoxy	10	0x10061fd0

Possible Origin

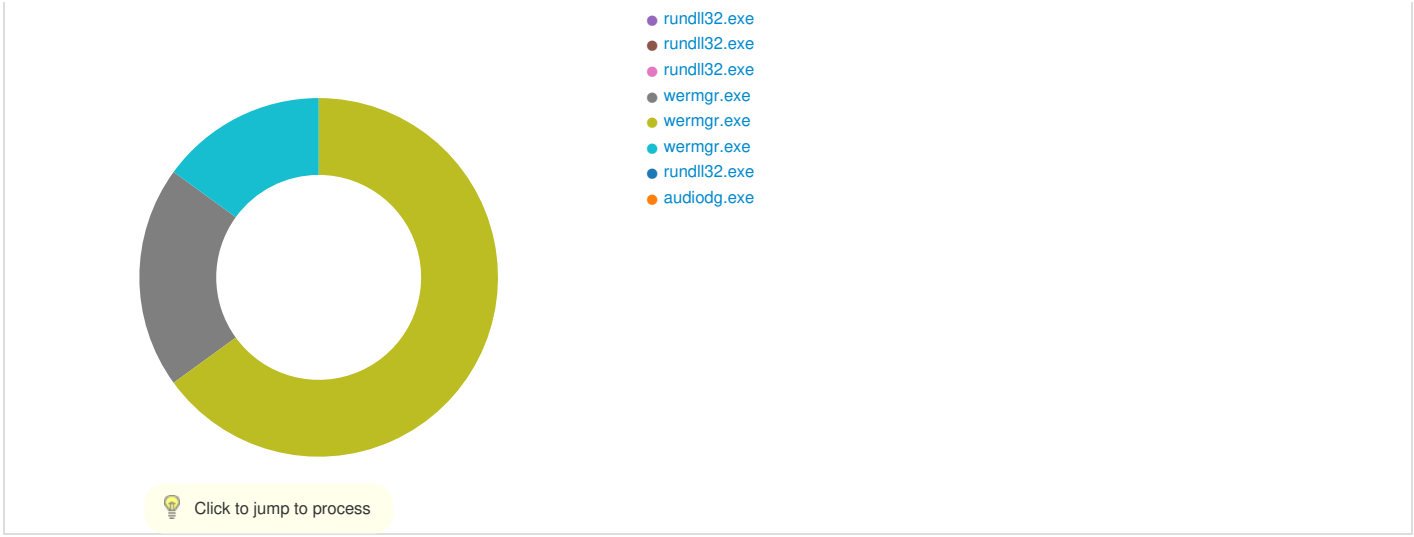
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5328, Parent PID: 3452

General

Target ID:	0
Start time:	17:39:50
Start date:	03/10/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\pebbles.dat.dll"
Imagebase:	0xb90000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5864, Parent PID: 5328

General

Target ID:	1
Start time:	17:39:50
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: cmd.exe PID: **5900**, Parent PID: **5328**

General

Target ID:	2
Start time:	17:39:51
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5696**, Parent PID: **5328**

General

Target ID:	3
Start time:	17:39:51
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\pebbles.dat.dll
Imagebase:	0xae0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000003.00000002.269120079.0000000000990000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000002.269120079.0000000000990000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000002.269120079.0000000000990000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000003.00000003.261366767.0000000000590000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000003.261366767.0000000000590000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000003.261366767.0000000000590000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5792**, Parent PID: **5900**

General	
Target ID:	4
Start time:	17:39:51
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.269061857.0000000004450000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000002.269061857.0000000004450000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000002.269061857.0000000004450000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000003.261746477.0000000004430000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000003.261746477.0000000004430000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000003.261746477.0000000004430000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: rundll32.exe PID: 5784, Parent PID: 5328

General	
Target ID:	5
Start time:	17:39:51
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllRegisterServer
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000003.261991952.0000000002D60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000003.261991952.0000000002D60000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000003.261991952.0000000002D60000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000002.268833263.0000000002EE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000002.268833263.0000000002EE0000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000002.268833263.0000000002EE0000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: rundll32.exe PID: **5360**, Parent PID: **5328**

General	
Target ID:	6
Start time:	17:39:54
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllUnregisterServer
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wermgr.exe PID: **4884**, Parent PID: **5792**

General	
Target ID:	7
Start time:	17:39:56
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1340000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000007.00000002.270568639.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000000.268101186.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000007.00000000.268101186.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000007.00000000.268101186.0000000000E40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\pebbles.dat.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f fd 10 08 1b fd 7e 5b 1b fd 7e 5b 1b fd 7e 5b fd fd 7d 5a 02 fd 7e 5b fd fd 7b 5a fd fd 7e 5b fd fd 7a 5a 03 fd 7e 5b 49 fd 7a 5a 14 fd 7e 5b 49 fd 7d 5a 08 fd 7e 5b 49 fd 7b 5a 58 fd 7e 5b fd fd 7f 5a 1c fd 7e 5b 1b fd 7f 5b 6f fd 7e 5b fd fd 77 5a 1c fd 7e 5b fd fd 7e 5a 1a fd 7e 5b fd c1 5b 1a fd 7e 5b 1b fd fd 5b 1a fd 7e 5b fd fd 7c 5a 1a fd 7e 5b 52 69 63 68 1b fd 7e	MZ@!L!This program cannot be run in DOS mode.$_~[~[~[}Z~[{Z~[zZ~[IzZ~[I}Z~[I{ZX~[Z~[[o~[wZ~[~Z~[[~[[~[|Z~[Rich~	success or wait	1	E4B4DE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\pebbles.dat.dll	unknown	493056	success or wait	2	E4B53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	E4B53C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	success or wait	1	E4AA0C	RegCreateKeyA

Analysis Process: wermgr.exe PID: **612**, Parent PID: **5784**

General

Target ID:	8
Start time:	17:39:56
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1340000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000008.00000000.268192549.00000000012A0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000008.00000000.268192549.00000000012A0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000008.00000000.268192549.00000000012A0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Created

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\Microsoft\Ikoqhruop</td><td>read data or list directory | synchronize</td><td>device</td><td>directory file | synchronous io non alert | open for backup ident | open reparse point</td><td>success or wait</td><td>1</td><td>12A3289</td><td>CreateDirectoryW</td></tr>
</table>

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\pebbles.dat.dll</td><td>0</td><td>4096</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f fd 10 08 1b fd 7e 5b 1b fd 7e 5b 1b fd 7e 5b fd fd 7d 5a 02 fd 7e 5b fd fd 7b 5a fd fd 7e 5b fd fd 7a 5a 03 fd 7e 5b 49 fd 7a 5a 14 fd 7e 5b 49 fd 7d 5a 08 fd 7e 5b 49 fd 7b 5a 58 fd 7e 5b fd fd 7f 5a 1c fd 7e 5b 1b fd 7f 5b 6f fd 7e 5b fd fd 77 5a 1c fd 7e 5b fd fd 7e 5a 1a fd 7e 5b fd c1 5b 1a fd 7e 5b 1b fd fd 5b 1a fd 7e 5b fd fd 7c 5a 1a fd 7e 5b 52 69 63 68 1b fd 7e</td><td>MZ@!L!This program cannot be run in DOS mode.$_~[~[~[}Z~[{Z~[zZ~[IzZ~[I}Z~[I{ZX~[Z~[[o~[wZ~[~Z~[[~[[~[|Z~[Rich~</td><td>success or wait</td><td>1</td><td>12AB4DE</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\pebbles.dat.dll	unknown	493056	success or wait	2	12AB53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	12AB53C	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	5d054d9	binary	37 85 E4 1E 1A 9B EA D2 7C C3 81 65 89 DC 1C 3A C3 88 65 34 0F 84 FA B9 16 C5 58 6D C6 9F CA	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	304f8497	binary	17 DA D1 FE B2 7A 00 78 53 02 38 B7 A5 81 73 7C 84 CA D8 6D A0 90 A7 F4 B9 A4 88 6E E2 EC 3C 32 84 F8 ED 20 B7 D2 90 EB A2 2A DB 93 77 A4 0E 5E 52 A6 31 F8 B3 C1 B3 6C 37 F3 BF 2A 7C 60 D4 D8 58 62 CE AA 08 09 60 A9 4A 8C 78 0F 9F AC FB 31 6A 47 33 BE FE E5 BF 1C B3 ED ED 61 25 C5 8C BE 56 F5 48 C6 40 C8 63 40 5A 6A D5 AD E1 94 3C F9 05 0C B7 A6 3C 7C 82 AC 19 01 F7 D1 E5 FE E2 D6 09 81 D9 3C 0B 92 17 1E 9B 6C 03 C1 03 6A 6A B2 F4 B1 ED 3C DA CB 94 33 66 19 BD 4B C7 EE 49 AE 8F 0E 65 87 0A 7B AE 7A E2 FF BD 11 5E 64 A3 80 31 B5 F9 44 64 11 4A 28 34 61 E7 64 C3	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	320ea4eb	binary	AE D0 75 18 4E 47 83 B6 C7 B3 1C BD 6E C1 9D E7 B3 99 9C AA D0 CE 25 35 9D A1 89 AD A1 6D FA 7E 5B 37 00 3D 65 A5 BF 74 0B 11 F3 FD 52 1B BC E4 27 CE 39 88 34 DA 18 86 B7 E5 48 18 AB 84 EF 2B 0F B2 64 17	success or wait	1	12AAF2F	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	8ab2c38e	binary	48 E9 AE AD 4C C9 33 72 6C CE 3A BC 62 B5 8D BC 70 92 68 D4 CF 92 A8 46 94 1F 7E 59 27 20 65 83 90 69 56 35 97 AD 82 3A 9A 7A 6D FE D0 45	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	f7ba8c04	binary	83 75 61 2D 03 C6 62 D8 79 E9 A4 61 3A 62 DF 38 C9 E2 AB 11 D3 32 AF DB 5D 6E 65 9A 43 4D 57 B1 D4 99 C5 F3 FD E4 B8 EA BC DE C3 46 A3 FD CA 5D 60 3D 00 3E 34 3E CB 68 A6 8B CC D6 8E 30 A5	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	4f06eb61	binary	31 D5 A5 19 DF 7B 74 69 67 E3 88 42 DE 98 29 0A BB 5D D2 06 76 D9 A7 99 2B E9	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	88f3e3f2	binary	C1 2B 0F D2 C1 CA 63 51 97 98 4C F5 70 13 3E 27 DC 8E 12 03 83 1E A8 1E FF A9 7D 12 F8 41 B9 45 4D 0D A7 B6 F6 7D 95 FE 99 5C 53 CF 78 E6 93 65 5B E7 F6 DA 8D 5F C4 42 57 5D 3A 68 4E B0 F6 94 31 BF 64 EC 8A 4B E2 5E 2D 83 DC 36 3D 46 7B 0C C5 9B 73 86 7B EB C3 22 BF 0C 68	success or wait	1	12AAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	7a993b2f	binary	F0 33 05 8E FA A5 91 26 4A 49 5A FC 65 A0 40 A1 1C 33 CD 61 EC 47 B7 1F 22 AE 79 91 9E 52 E4 C8 43 D5 E2 E5 90 D5 E2 21 32 3B 57 AB F6 C3 D1	success or wait	1	12AAF2F	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ymxempiiozk	5d054d9	binary	37 85 E4 1E 1A 9B EA D2 7C C3 81 65 89 DC 1C 3A C3 88 65 34 0F 84 FA B9 16 C5 58 6D C6 9F CA	37 85 F3 1E 1A 9B D9 CE D8 DE A5 AE 87 5D C8 35 38 75 6E E2 3F EC 0C A0 AF 79 65 85 D2 49 A7 D6 ED A5 85 4A 7B D6 9B 99 AE 7D FF 92 E2 1F 59 0C 1F C1 AE 0B	success or wait	1	12AAF2F	RegSetValueExA

Analysis Process: wermgr.exe PID: **3472**, Parent PID: **5696**

General

Target ID:	9
Start time:	17:39:56
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1340000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000002.270604125.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000009.00000002.270604125.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000009.00000002.270604125.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000000.268299338.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000009.00000000.268299338.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000009.00000000.268299338.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\pebbles.dat.dll	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f fd 10 08 1b fd 7e 5b 1b fd 7e 5b 1b fd 7e 5b fd fd 7d 5a 02 fd 7e 5b fd fd 7b 5a fd fd 7e 5b fd fd 7a 5a 03 fd 7e 5b 49 fd 7a 5a 14 fd 7e 5b 49 fd 7d 5a 08 fd 7e 5b 49 fd 7b 5a 58 fd 7e 5b fd fd 7f 5a 1c fd 7e 5b 1b fd 7f 5b 6f fd 7e 5b fd fd 77 5a 1c fd 7e 5b fd fd 7e 5a 1a fd 7e 5b fd c1 5b 1a fd 7e 5b 1b fd fd 5b 1a fd 7e 5b fd fd 7c 5a 1a fd 7e 5b 52 69 63 68 1b fd 7e	MZ@!L!This program cannot be run in DOS mode.$_~[~[~[}Z~[{Z~[zZ~[lzZ~[l}Z~[l{ZX~[Z~[[o~[wZ~[~Z~[[~[[~[|Z~[Rich~	success or wait	1	97B4DE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\pebbles.dat.dll	unknown	493056	success or wait	2	97B53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	97B53C	ReadFile

Analysis Process: rundll32.exe PID: **5580**, Parent PID: **5328**

General

Target ID:	10
Start time:	17:39:57
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,bewailable
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: audiodg.exe PID: **3472**, Parent PID: **1640**

General

Target ID:	33
Start time:	17:42:12
Start date:	03/10/2022
Path:	C:\Windows\System32\audiodg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\AUDIODG.EXE 0x2ac
Imagebase:	0x7ff724e50000
File size:	594128 bytes
MD5 hash:	0B245353F92DF527AA7613BA2C0DA023
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly