ID: 715156
Sample Name: pebbles.dat.dll
Cookbook: default.jbs
Time: 17:26:43
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

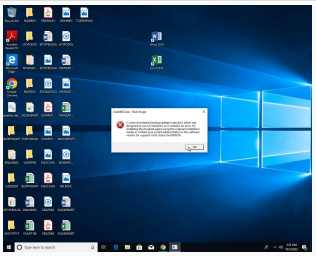
Windows Analysis Report

pebbles.dat.dll

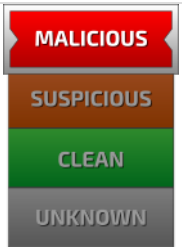
Overview

General Information

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



Detection



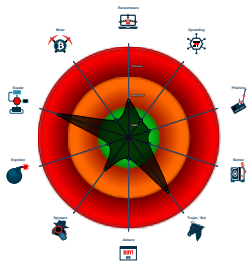
Qbot

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: 5860 cmdline: loaddll32.exe "C:\Users\user\Desktop\pebbles.dat.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5896 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5916 cmdline: rundll32.exe "C:\Users\user\Desktop\pebbles.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - wermgr.exe (PID: 5996 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - regsvr32.exe (PID: 5904 cmdline: regsvr32.exe /s C:\Users\user\Desktop\pebbles.dat.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - wermgr.exe (PID: 5988 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 5924 cmdline: rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6004 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 5968 cmdline: rundll32.exe C:\Users\user\Desktop\pebbles.dat.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6040 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
00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.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

Source	Rule	Description	Author	Strings
00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.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
00000004.00000003.245679829.00000000032E0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000003.245679829.00000000032E0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x1034f:$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
8.2.wermgr.exe.2d40000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
8.2.wermgr.exe.2d40000.0.raw.unpack	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x10f4f:$a: 33 C0 59 85 F6 74 2D 83 66 0C 00 40 89 06 6A 20 89 46 04 C7 46 08 08 00
8.2.wermgr.exe.2d40000.0.raw.unpack	Windows_Trojan_Qbot_3074a8d4	unknown	unknown	• 0x1ca14:$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:$generate_random_alpha_num_string: 57 E8 DC DC FF FF 48 50 8D 85 30 F6 FF FF 6A 00 50 E8 D1 6D 0 0 00 8B 4D F8 83 C4 10 8A 04 38 88 04 0E 46 83 FE 0C
8.0.wermgr.exe.2d40000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
8.0.wermgr.exe.2d40000.0.unpack	Windows_Trojan_Qbot_92c67a6d	unknown	unknown	• 0x1034f:$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

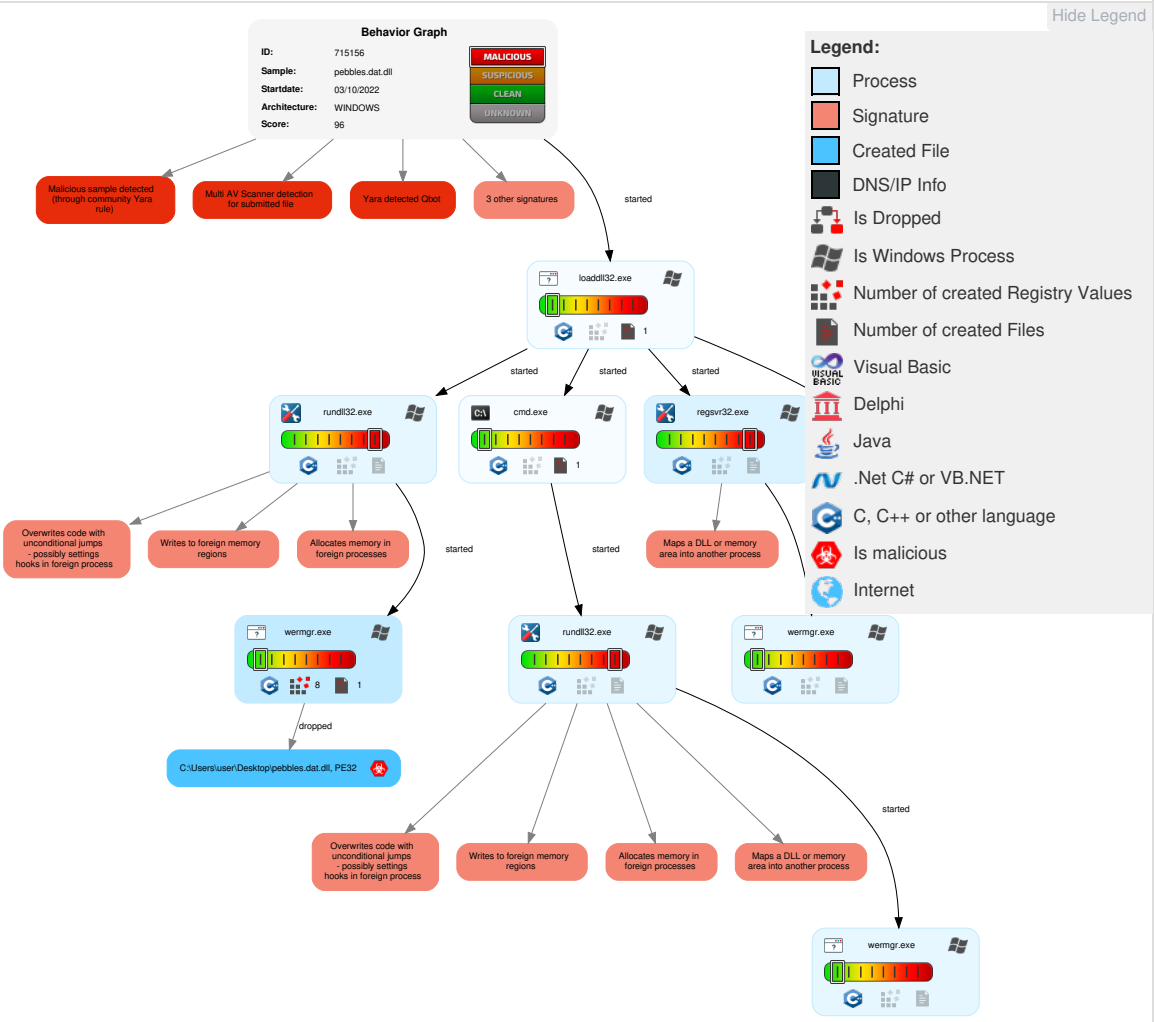
Yara detected Qbot

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

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

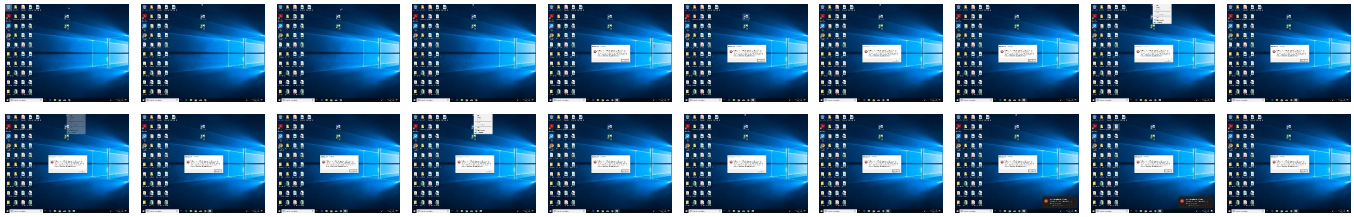
Behavior Graph

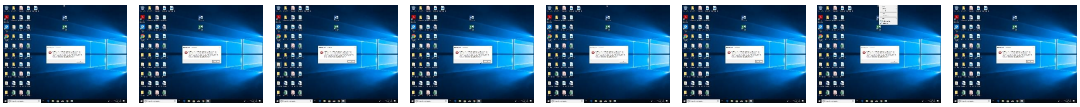


Screenshots

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
4.2.rundll32.exe.3460000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
5.2.rundll32.exe.4a60000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
3.2.regsvr32.exe.3160000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Source	Detection	Scanner	Label	Link	Download
8.2.wermgr.exe.2d40000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
7.0.wermgr.exe.2c60000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
8.0.wermgr.exe.2d40000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
7.2.wermgr.exe.2c60000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
9.0.wermgr.exe.29b0000.0.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 17:26:43 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
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
Number of analysed new started processes analysed:	22
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@20/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.4% (good quality ratio 24.2%) • Quality average: 77.4% • Quality standard deviation: 26%

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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.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

Time	Type	Description
17:27:47	API Interceptor	9x Sleep call for process: wermgr.exe modified

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 00007F5C910C8327h

Instruction
call 00007F5C910C8844h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F5C910C81D3h
add esp, 0Ch
pop ebp
retn 000Ch
cmp ecx, dword ptr [10001D84h]
jne 00007F5C910C8323h
ret
jmp 00007F5C910C892Dh
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

Instruction
int3
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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

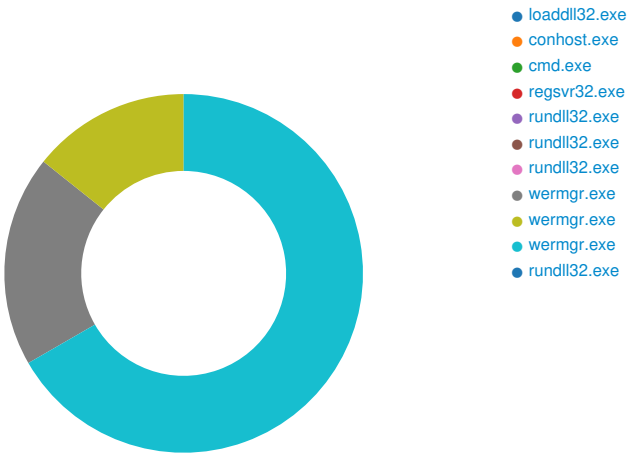
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **5860**, Parent PID: **3320**

General

Target ID:	0
Start time:	17:27:36
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:	0x1200000
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: **5868**, Parent PID: **5860**

General

Target ID:	1
Start time:	17:27:37
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **5896**, Parent PID: **5860**

General

Target ID:	2
Start time:	17:27:37
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:	0xa60000
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: **5904**, Parent PID: **5860**

General

Target ID:	3
Start time:	17:27:37
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:	0x8c0000
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: 00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000002.252637894.0000000003160000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000003.00000003.245541502.0000000003140000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000003.00000003.245541502.0000000003140000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000003.00000003.245541502.0000000003140000.00000004.00000800.00020000.00000000.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: **5916**, Parent PID: **5896**

General	
Target ID:	4
Start time:	17:27:37
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:	0x1280000
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: 00000004.00000003.245679829.00000000032E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000003.245679829.00000000032E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000003.245679829.00000000032E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.252645898.0000000003460000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000004.00000002.252645898.0000000003460000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000004.00000002.252645898.0000000003460000.00000040.00000800.00020000.00000000.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: 5924, Parent PID: 5860

General	
Target ID:	5
Start time:	17:27:37
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:	0x1280000
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: 00000005.00000002.252831702.0000000004A60000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000002.252831702.0000000004A60000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000002.252831702.0000000004A60000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000003.246084770.0000000004A40000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000005.00000003.246084770.0000000004A40000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000005.00000003.246084770.0000000004A40000.00000004.00000800.00020000.00000000.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: **5968**, Parent PID: **5860**

General	
Target ID:	6
Start time:	17:27:40
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:	0x1280000
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: **5988**, Parent PID: **5904**

General	
Target ID:	7
Start time:	17:27:43
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x970000
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: 00000007.00000000.251843249.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000007.00000000.251843249.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000007.00000000.251843249.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000002.254795791.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000007.00000002.254795791.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000007.00000002.254795791.0000000002C60000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

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	2C6B4DE	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	2C6B53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	2C6B53C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	success or wait	1	2C6AA0C	RegCreateKeyA

Analysis Process: wermgr.exe

PID: **5996**, Parent PID: **5916**

General

Target ID:	8
Start time:	17:27:43
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x970000
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: 00000008.00000002.254770959.000000002D40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000008.00000002.254770959.000000002D40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000008.00000002.254770959.000000002D40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000008.00000000.251930910.000000002D40000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000008.00000000.251930910.000000002D40000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000008.00000000.251930910.000000002D40000.00000040.80000000.00040000.00000000.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~[[~[[~[lZ~[Rich~	success or wait	1	2D4B4DE	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	2D4B53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	2D4B53C	ReadFile

Analysis Process: wermgr.exe PID: **6004**, Parent PID: **5924**

General

Target ID:	9
Start time:	17:27:43
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x970000
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: 00000009.00000000.252174416.00000000029B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Qbot_92c67a6d, Description: unknown, Source: 00000009.00000000.252174416.00000000029B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Qbot_3074a8d4, Description: unknown, Source: 00000009.00000000.252174416.00000000029B0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Qyioamjyn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	29B3289	CreateDirectoryW

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 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	29BB4DE	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	29BB53C	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	29BB53C	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	dbdf127f	binary	30 C7 DF 0A BE FA DA AB 0A C1 C7 44 C3 01 06 D8	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	ee40c231	binary	4A B5 4C C4 AE 51 F4 F9 5B 49 1B A5 3F 70 BD D2 44 5A 03 13 7E 2F 51 41 E7 B9 03 14 64 BB 1A B1 48 B6 D1 7E 5F A4 EE C7 6D 3E 25 A9 D5 44 0F 31 E4 F3 D4 B8 7F F8 5F AB EE 02 56 02 58 59 3C D7 DA 58 4B C1 7B EB DE BF 6F 98 64 A8 EE 1B 06 3C CB 4B 67 0E C5 7A 86 BE 04 32 CB 8A 01 64 70 95 1D DD EE 07 FF 35 31 88 7A A4 7D CB E3 83 FD 5E 51 E5 D7 D6 3D AD 4E 64 93 6B 3E C3 24 76 DF CD F5 77 B5 EF 2F CE 1C 1B BB 51 55 82 B3 DC DC 9B 32 C2 6D 9A 13 45 DD FE 51 0B CC 62 45 27 EB AE 3B 3F 74 07 88 CF F1 A6 F2 7F F5 43 1F 4D	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	ec01e24d	binary	EA 41 3D 5B 71 FB 9A EE 31 4A A7 98 12 A9 99 29 C2 B3 28 E7 69 CB C9 3E 99 4A DA 7C 38 A4 D1 A0 AD A8 68 73 4B E2 ED D7 03 25 87 57 F8 C7 37 1D AD 8D 53 53 4A 25 9D ED 54 24 5C	success or wait	1	29BAF2F	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	54bd8528	binary	91 58 FA 5F 1D 96 D0 FB FB E3 98 EF 0D 89 69 F6 78 A9 92 0F 05 5F 71 0D 62 24 9B 6A 15 22 55 22 12 1B 51 A4 CE 9D C1 A0 1C 54 36 75 1B 20 83 30 80 F1 88 64 2E D9 BB FF 95 92 08 D4 8A 09 B8 AB 96 48 9E AD 9F FF F1 12 0F 89	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	29b5caa2	binary	C3 91 1F 92 DD 63 39 D3 5F C7 DE 23 06 4B 71 8E 79 E0 BA 25 15 E1 64 43 E2 42 49 F0 1D F6 89 0E BC BF 26 DF 86 53 0C 83 A1 72 42 9B FE 0C 18 96 C0 73 A7 A5 32 39 E9 99 73 BF D6 89 FB 54 EC A8 F0 1A 76 C7 D2 F5 F8 D3 58 64 3D 4E 07 68 6B A6 2D 43 7C 52 F9 B4 0D 4B B3 B6 9C 17 62 EE 26 EF 7C FC 8A 08 6B 7D 08 BB B6 6B A3 70 31 B9 5B CA D9	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	9109adc7	binary	26 07 22 6F AF 55 B9 BA 3F 70 0D 35 A5 9F 74 04 9F 8B 11 4A 7D C5 04 2F 2D 9B D1 05 DB 77 D2 B9 0C EA 89 BC F3 92 48 79 E7 3F 69 A3 CA 4A D4 DE 77 A0 63 A2 C5 E6 C5 3D 37 76 46 52 7B E6 CC A5 40 C8 FE 8D 6A DE AB 58 FF 64 53 06 50 5E 47 5F DA D0 DB 18 BD 70 C3 BA 0C C2 4D FF 17 CA 0E 1D 6F E0 4F A3 63 D4 4E 0E	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	56fca554	binary	5B 83 D1 C5 26 1E 1D 05 CC 28 71 64 62 BB A8 F7 79 79 84 D1 FF 23 5B 30 57 B0 3C 18 48 34 13 96 8C E6 43 49 AE 17 1A 85 D2 34 CA 0D F6 C7 D8 AD BA 34 A3	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	a4967d89	binary	8B A5 4F 62 29 54 0D 59 01 0B D4 9E 3B AE 89 8A 8E CA FE A3 73 94 C9 FE 43 D3 EC C1 CE E4 56 F3 46 05 AC 04 B7 7A B2 DF 20 B3 AF 0F F1 72 6D 0F 81 12 83 0B 72 73 65 EB 0A 9E 8A 53 45 0B DB FA EA 43 DD 93 5E 60 C2 8E 4E AF C9 B4 00 11 BB 7D 28 4D B6 FB 0A FE 9B 14 88 5E 63 DE FA 8B 89 9A F0 7F	success or wait	1	29BAF2F	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	dbdf127f	binary	30 C7 DF 0A BE FA DA AB 0A C1 C7 44 C3 01 06 D8	30 C7 C8 0A BE FA E9 AC 57 01 F8 CE D3 B7 3D 39 1C A8 24 B4 72 B5 D2 43 7E 54 1C FE 2B 87 F1 D3 AE 83 CF DA 8C	success or wait	1	29BAF2F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Rqqahuvpx	dbdf127f	binary	30 C7 C8 0A BE FA E9 AC 57 01 F8 CE D3 B7 3D 39 1C A8 24 B4 72 B5 D2 43 7E 54 1C FE 2B 87 F1 D3 AE 83 CF DA 8C	30 C7 C8 0A BE FA E9 AC 57 01 F8 CE D3 B7 3D 39 1C A8 24 B4 72 B5 D2 43 78 5A 1D FE 2B 87 F1 D3 AE 83 CF DA 8C	success or wait	1	29BAF2F	RegSetValueExA

Analysis Process: rundll32.exe PID: **6040**, Parent PID: **5860**

General

Target ID:	10
Start time:	17:27:44
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:	0x1280000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

No disassembly