ID: 452460
Sample Name: PRTService.exe
Cookbook: default.jbs
Time: 12:04:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

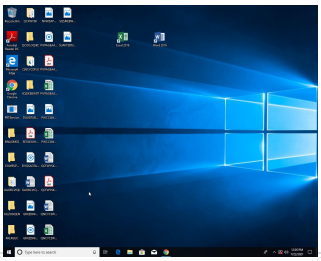
Windows Analysis Report PRTService.exe

Overview

General Information

Sample Name:	PRTService.exe
Analysis ID:	452460
MD5:	4a838989da416e..
SHA1:	f2fb096d74527a0..
SHA256:	26c2caf1eb317e9..
Infos:	

Most interesting Screenshot:



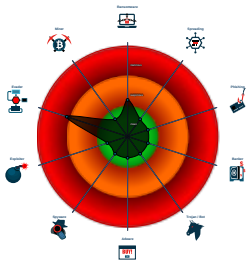
Detection

Score:	26
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Tries to detect virtualization through…
- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to dynamically…
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function
- Drops PE files
- One or more processes crash
- PE file contains sections with non-s…
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (

Classification



Analysis Advice

Sample crashes during execution, try analyze it on another analysis machine

Sample may be VM or Sandbox-aware, try analysis on a native machine

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Process Tree

- **System is w10x64**
- PRTService.exe (PID: 5480 cmdline: 'C:\Users\user\Desktop\PRTService.exe' MD5: 4A838989DA416E3D16C520D03C3BA192)
  - dw20.exe (PID: 5976 cmdline: dw20.exe -x -s 852 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

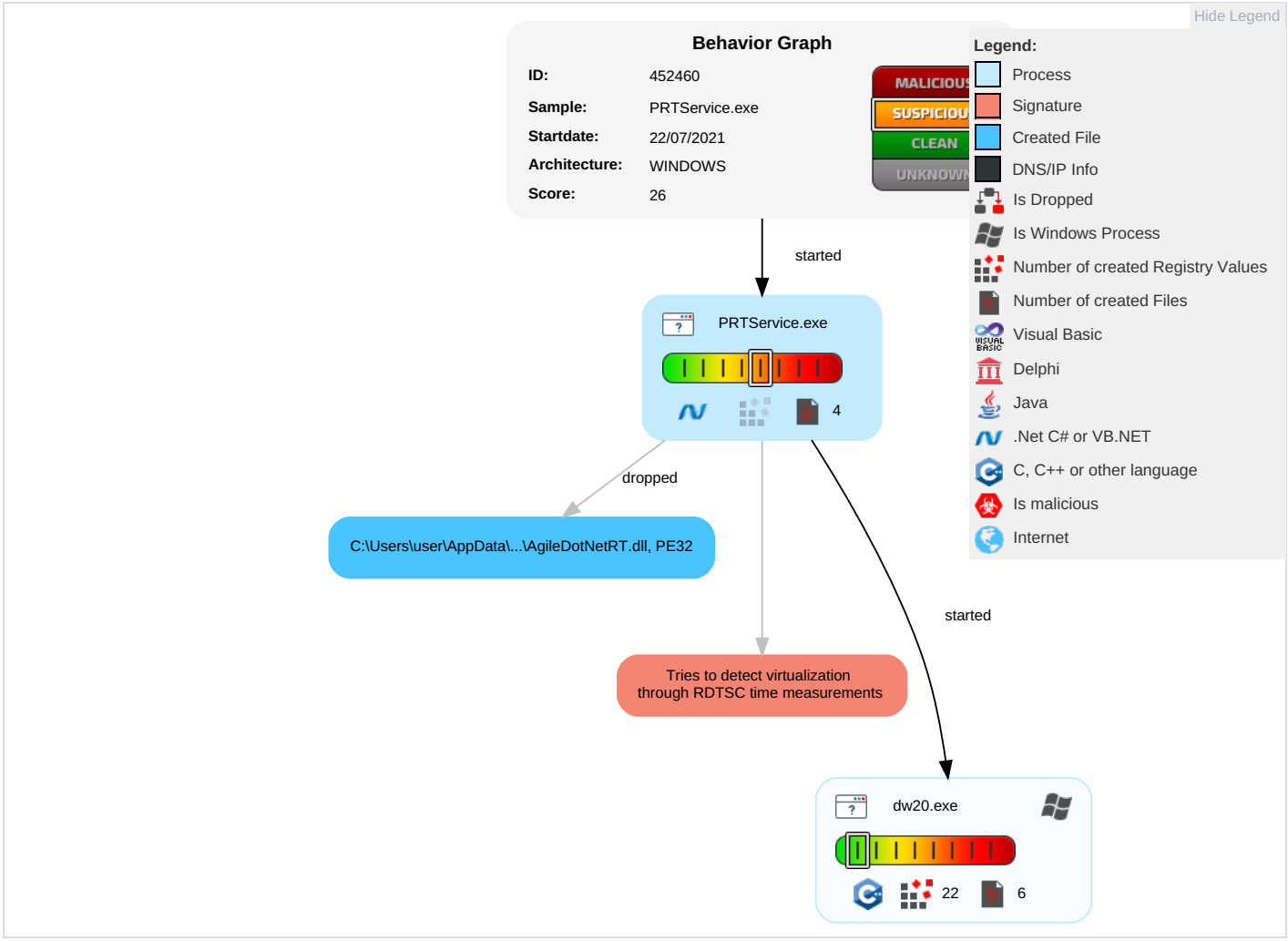
Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T V A
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	C D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
PRTService.exe	6%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1d7a2c72-3aee-4299-91f8-2280595a512b\AgileDotNetRT.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\1d7a2c72-3aee-4299-91f8-2280595a512b\AgileDotNetRT.dll	2%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1d7a2c72-3aee-4299-91f8-2280595a512b\AgileDotNetRT.dll	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452460
Start date:	22.07.2021
Start time:	12:04:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRTService.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:	3
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:	SUS
Classification:	sus26.evad.winEXE@3/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 68% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:04:59	API Interceptor	1x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_prtservice.exe_9a52ed83f9a038e8d5d8a8b157025a4bf964059_00000000_170c17b5\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	3.77494316680188
Encrypted:	false
SSDEEP:	192:qukBTvHiNmXmhnZaKsn9fXeewQlfY/u7s6S274ltxUn:r2TiraDfY/u7s6X4ltW
MD5:	BC1FC11A79D4F343E5BB91CE09B7E8AD
SHA1:	D7B371EAEFB34AF61C2D839AB37529D9ACBFB38E
SHA-256:	157F9E47E5C2B3807B350974B124C7F32129A991AD8B1F8092B3D33CCE9EA5CF
SHA-512:	460570B46667510C06D40CAAD8B61EF7B8444A4BB13DC899DA97C5D9ED2B5C30582A2B5EEBA13B980B7D66A68DDB87309B8CC133EE274F3233335C95A71AE52
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.1.4.5.4.2.9.7.2.5.0.4.9.2.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.1.4.5.4.2.9.7.5.4.7.3.8.4.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.a.a.9.f.8.6.7.-.5.c.8.2.-.4.4.6.3.-.9.4.7.f.-.3.1.8.b.e.5.8.7.b.9.f.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.R.T.S.e.r.v.i.c.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.6.8.-.0.0.0.1.-.0.0.1.7.-.9.8.a.3.-.4.c.7.5.2.c.7.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.d.4.4.3.3.7.a.a.a.c.6.2.e.9.a.f.7.2.5.a.0.b.2.6.a.b.f.5.d.7.3.0.0.0.0.0.0.0.0.!.0.0.0.0.f.2.f.b.0.9.6.d.7.4.5.2.7.a.0.6.c.5.b.5.c.2.9.7.5.f.d.4.3.8.4.1.9.e.c.1.7.1.b.6.!.P.R.T.S.e.r.v.i.c.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.1.7././.1.1././.2.9.:.2.0.:.0.9.:.3.3.!.0.!.P.R.T.S.e.r.v.i.c.e...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	3.696497169104449
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNik6U6ksMe6YSKSUNC1lgmfZJAdS+Cp1yb1fYqGm:RrlsNil696YfSUNC1lgmfXOSnypfr
MD5:	1EBF2F48397EFDD1021EDE3AF4B317DC
SHA1:	48847211A8D7E6385E13908B6F951483DDAD5AED
SHA-256:	55ABEF9712C023C23556FBE0439396D36F9626F229BB144475BAB8A1FAEAD0FD
SHA-512:	F9E1F2EA19AE2BFE6C7814B6F27748C16DAA0C423AFEEB02EC845E1198C7B6D5038D844AC0C26361F5D269DFDCB18055703268F3475D21C058AE48BD7868A782
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC2.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE60.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4699
Entropy (8bit):	4.4714599202674306
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9ZVWSC8Bhs8fm8M4JFKzLtJ2F3f+q8vCLtJfebF9pd:uITfR6kSNbRJFKsfKMep9pd
MD5:	BF3AD03AC5C53F7BD1E72D3B3BB4C4E1
SHA1:	3F8D93C4AEECFE1BFC18E53DC9C758F6AC7D3E8B
SHA-256:	80E099F69D975A62E4B82EC1E9AD616938D4A425EE51BB4EDAB3E5EABEFB49D1
SHA-512:	494C602BD5A3ACDAA155379483A070611E77772F1A54B2A7339E106025A145829FC2785E7888F2A8D8457A6D6764C80DDDA5AEBF0F5D11CDFE625120127BA7E5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1088895" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\1d7a2c72-3aee-4299-91f8-2280595a512b\AgileDotNetRT.dll	
Process:	C:\Users\user\Desktop\PRTService.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123285
Entropy (8bit):	6.470545105128027
Encrypted:	false
SSDEEP:	3072:eoVfy2n+bR4l+w5wlDn+1HcR6bpMpImsGPZni2:ly2n+bR42xcR6bpUxni2
MD5:	F377D15AD215C779E12775DE2B42C965
SHA1:	59409AC15E0535CEA47EC5AC5968867E8FF8C0E6
SHA-256:	BC2440A2A185006247BE562F4D6B67560309E48694CC854308E00C41F02CA7D8
SHA-512:	11AFDD6F098AB7D7466A764868D9E163142836B11044A0A2572EAC305454328B6FADE08929F93BD9E5FA9436435C5566A3C2EE86F1CDA6457B908F1198E22CF1
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F...F...F..TF...F..lF...F...F...F..aF...F.wTF...F.wdF...F.weF...F.wbF...FRich...F.....PE..L....9VS.....!.....8..... .....|....@.....#.....@..d...`.....p.....B.....P..`.....textbss.....text...)..... ..`.rdata.....@..@.data.....0.....@....idata.....@.....@....didata.....P.....*.....@....rsrc.....`.....@..@.reloc.....p.....2.....`.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.818104665244162
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.69% • Win32 Executable (generic) a (10002005/4) 49.65% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • InstallShield setup (43055/19) 0.21% • Windows Screen Saver (13104/52) 0.07%
File name:	PRTService.exe

General

File size:	957952
MD5:	4a838989da416e3d16c520d03c3ba192
SHA1:	f2fb096d74527a06c5b5c2975fd438419ec171b6
SHA256:	26c2caf1eb317e9354cec8a92e824a495ce7d253f6d1779226138e6994553cf9
SHA512:	ab62430a4d72f4e6d71c489fe45e338a8b877f5d9936bd10ea60a6d325fa02e03d25652a04a3262fcff8347e121fee876b4b98c8f767f5339ba8c01c1d0d9f9c
SSDEEP:	12288:4BnFzJLhIE3wD2gM+L+GQtXJoqWJ+7MVOIVcD:cFprPDtPW87MVOs8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Z.....z.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4eb17a
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:	0x5A1F13FD [Wed Nov 29 20:09:33 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0xe9240	0xe9400	False	0.431423960008	data	6.82449258024	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xec000	0x54c	0x600	False	0.391927083333	data	3.95297327924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xee000	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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PRTService.exe PID: 5480 Parent PID: 5724

General

Start time:	12:04:55
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\PRTService.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRTService.exe'
Imagebase:	0xec0000
File size:	957952 bytes
MD5 hash:	4A838989DA416E3D16C520D03C3BA192
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dw20.exe PID: 5976 Parent PID: 5480

General

Start time:	12:04:56
Start date:	22/07/2021

Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 852
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis