ID: 502672
Sample Name: EDG.exe_
Cookbook: default.jbs
Time: 08:49:46
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

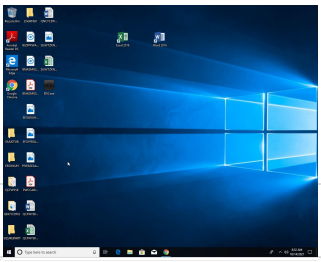
Windows Analysis Report EDG.exe_

Overview

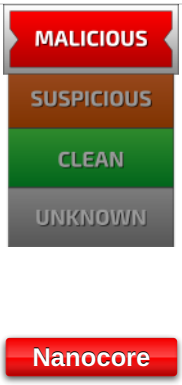
General Information

Sample Name:	EDG.exe_ (renamed file extension from exe_ to exe)
Analysis ID:	502672
MD5:	ad48c92ac820be..
SHA1:	39689d11546538..
SHA256:	22717cc02b1025..
Infos:	

Most interesting Screenshot:



Detection

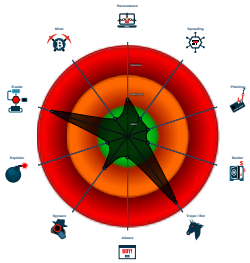


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- EDG.exe (PID: 2880 cmdline: 'C:\Users\user\Desktop\EDG.exe' MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
  - EDG.exe (PID: 6208 cmdline: C:\Users\user\Desktop\EDG.exe MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
    - schtasks.exe (PID: 5528 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD97B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6664 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDDF0.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- EDG.exe (PID: 4848 cmdline: C:\Users\user\Desktop\EDG.exe 0 MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
  - EDG.exe (PID: 6828 cmdline: C:\Users\user\Desktop\EDG.exe MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
- dhcpmon.exe (PID: 1744 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
  - dhcpmon.exe (PID: 7060 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
- dhcpmon.exe (PID: 3424 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
  - dhcpmon.exe (PID: 3460 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
  - dhcpmon.exe (PID: 6680 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: AD48C92AC820BE7297E6445E9CFEC1C0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "34cd1eb8-e195-44b9-a620-f386babd",
  "Group": "Default",
  "Domain1": "watermalon1.sytes.net",
  "Domain2": "",
  "Port": 7156,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.355181665.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000002.355181665.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000016.00000002.355181665.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000007.00000002.551341955.000000000620000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.551341955.000000000620000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost

Click to see the 58 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.EDG.exe.3bd05dc.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.EDG.exe.3bd05dc.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.EDG.exe.3bd05dc.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.2.EDG.exe.3bd4c05.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x24160:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x2418d:$x2: IClientNetworkHost
7.2.EDG.exe.3bd4c05.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x24160:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x2523b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x2417a:$s5: IClientLoggingHost
Click to see the 141 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

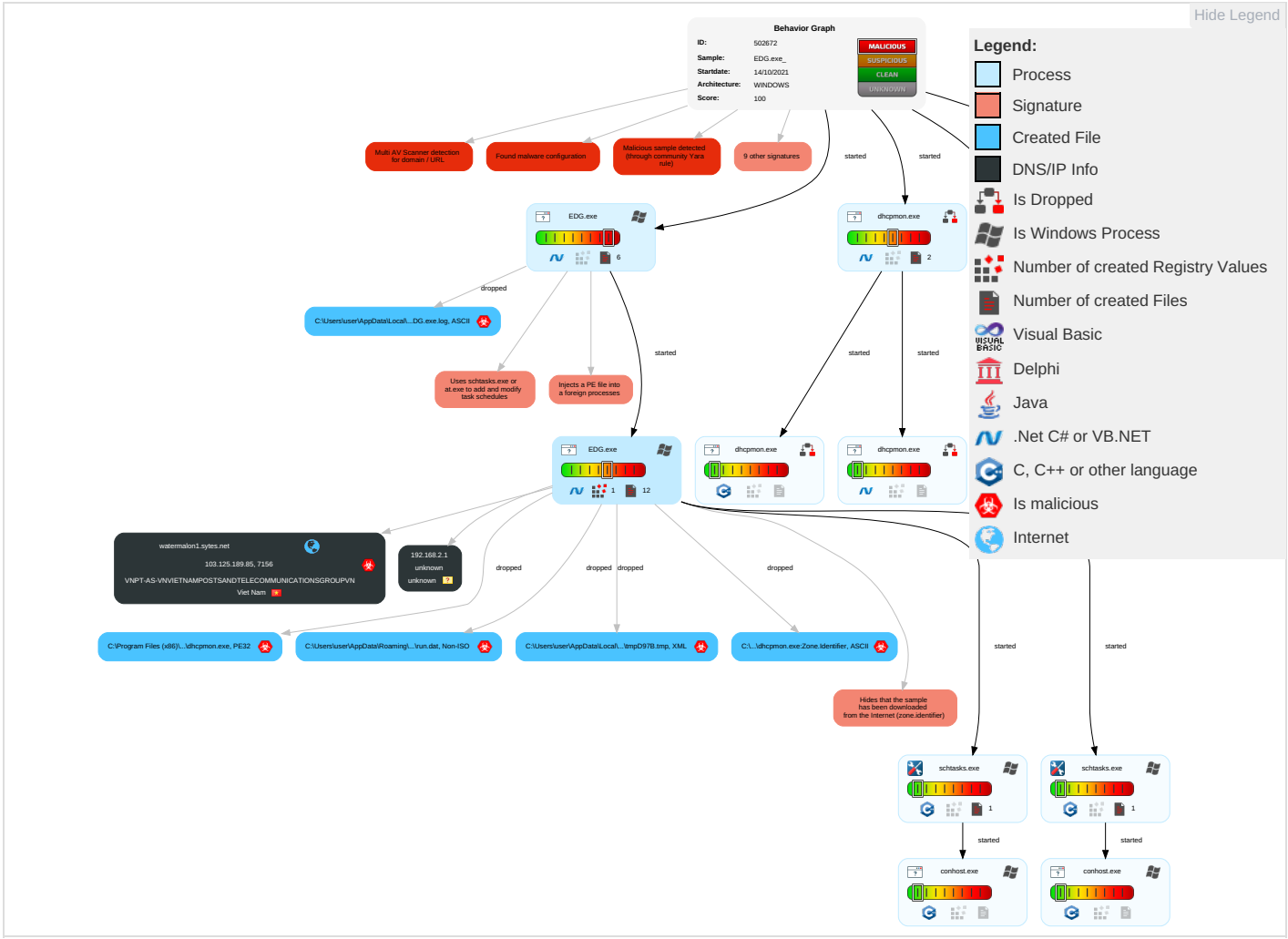
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

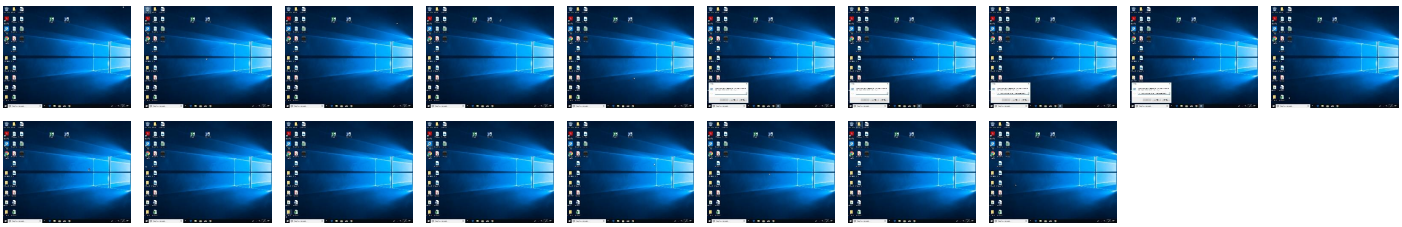
Behavior Graph



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
EDG.exe	24%	Virustotal		Browse
EDG.exe	33%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	24%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	33%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.EDG.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.EDG.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.EDG.exe.6250000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
watermalon1.sytes.net	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
watermalon1.sytes.net	11%	Virustotal		Browse
watermalon1.sytes.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
watermalon1.sytes.net	103.125.189.85	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
watermalon1.sytes.net	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.125.189.85	watermalon1.sytes.net	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502672
Start date:	14.10.2021
Start time:	08:49:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EDG.exe_ (renamed file extension from exe_ to 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/8@7/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0%) • Quality average: 11.9% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:50:44	API Interceptor	964x Sleep call for process: EDG.exe modified
08:50:51	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\EDG.exe" s>$(Arg0)
08:50:51	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:50:53	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:50:55	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	New Order For Chile.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	Polyvim LLC ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	cCA0tC5xHG	Get hash	malicious	Browse	• 14.225.54.71
	dringende begroting.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	4eB1luja0v	Get hash	malicious	Browse	• 14.225.234.63
	DHLAWB 191021.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	SZIJ791077 Brazil.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	5KnD4PBdwg.exe	Get hash	malicious	Browse	• 103.133.110.241
	5KnD4PBdwg.exe	Get hash	malicious	Browse	• 103.133.110.241
	5400040115 Pratincole Pacific PRAT-RR-21-H070 DELMAR MARINE SERVICES PTE LTD.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	5400040115 Pratincole Pacific PRAT-RR-21-H070 DELMAR MARINE SERVICES PTE LTD.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	dYBr3gE1a5.exe	Get hash	malicious	Browse	• 103.151.125.125
	3tpLnyN6Gl.exe	Get hash	malicious	Browse	• 103.151.125.125
	SHIPMENT DOCUMENTS.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	attached_wire_transfer_slip.xlsx	Get hash	malicious	Browse	• 103.145.254.169
	request list.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	attached wire transfer slip.xlsx	Get hash	malicious	Browse	• 103.145.254.169

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	518144
Entropy (8bit):	7.538455718497943
Encrypted:	false
SSDEEP:	6144:B1PHYG9KkdhRgyGzlYFVXzHlQnOhiyWTKF2DiWAjMTqvFSTixno2EfMkhB5FYB:nYyvd3aY7GOcy9oidjMutJ6+SB56
MD5:	AD48C92AC820BE7297E6445E9CFEC1C0
SHA1:	39689D11546538E304754A31C27973AA2E1B3CDE
SHA-256:	22717CC02B102548A6B9CDD13AD6F39E3282BEBD540138D5ACABEA80C8F71A01
SHA-512:	6AFEEC1830D13E7A36137B636C05CF4F4B90F8D67424207BD31E4D52EA175F21584EE72636E87BF1F72A394A9CD1295CDD802752D6D588D07C21030080A96C3
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r.fa.....0..V.....u... .....@.. .....@..... ..@.....Lu..O..... ....H.....text....U... ...V..... ..`.rsrc.....X.....@..@.rel oc..... .....@..B.....u.....H.....Lb..pO.....Y.....0..V.....}.....*.*s...}.....}.....}.....(.....(.....{....r...po.....{....r...po.....*...0..... .....(....&.{.....,...8....sA...%.{.....|....(....Z.{.....|....(....Z . &.s....} ...%.}.....{ ...(.....(....o.....+c...+C.....X.].....,+..(.....{....Z...{....Z.{....{....o .....X.....|....(.....-....X.....|....(. .....-.....,...o!.....sB.....|....(.....|....(....s"

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EDG.exe.log	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C 21
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C: \Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4 .0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5 61934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C 21
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows

C:\Users\user\AppData\Local\Temp\tmpD97B.tmp	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	5.101528053334886
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mxtn:cbk4oL600QydbQxIYODOLedq3Hj
MD5:	9B312DC553D9359743C79DE68B7C6C5A
SHA1:	EC296B038264BD26F8D8EAF6012D39A2B01DDB08
SHA-256:	31974160BA47DA068665E52BA8D9D54CE798090F0BC73DBD2C538100AB3D1461
SHA-512:	CD4E4D4A2C8B56E01454125164B4A5E9EDF54A786A1AB3586F335DF4CB536CA6D30D7A9D1601AF8BD9CF26CF733EB241AAEF4EE70236969DAD9919D43F0449F
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpDDF0.tmp	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:W2c:W2c
MD5:	63456BE972388D1CC2FC973CE0D600DB
SHA1:	02050D3926D8484C8CC6701A9FAF55C744AE1F7D
SHA-256:	8A9E638CFAF6A87718776395655CFEF0DF361112E9F8FDCFCE750FE15E1CA911
SHA-512:	525C860FE10E1EEC8B4CBDE0F957DBDFD29AB3015F2102736EC534152A072189DE6CADEAAFE07E1A019F0A1A6E47A13865060E32C837E8CE41251F04BB442EC
Malicious:	**true**
Preview:	.(.c*..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\EDG.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	4.081727678869736
Encrypted:	false
SSDEEP:	3:oNWXp5vghikA:oNWXpFghfA
MD5:	E36CE3A86A5425376A576FDD38F9B814
SHA1:	A0811E3F78140A29A9BFF3CDB0BCADDB8AB9830D
SHA-256:	663D083DFD035E2BA3AC03FC02957C6E3E7AA23AFE7E95A27D4478203DD43EEB
SHA-512:	3133B364A6CAAE2B66901BBA2413FD8F3AAEBFC60C5674358B6C1BB1DB6BF99822ACE67B66D567C3973CA315B8775BDA0A865624410574868F6014D0B6F98C4
Malicious:	false
Preview:	C:\Users\user\Desktop\EDG.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.538455718497943
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	EDG.exe
File size:	518144
MD5:	ad48c92ac820be7297e6445e9cfec1c0
SHA1:	39689d11546538e304754a31c27973aa2e1b3cde
SHA256:	22717cc02b102548a6b9cdd13ad6f39e3282bebd540138d5acabea80c8f71a01
SHA512:	6afeec1830d13e7a36137b636c05cf4f4b90f8d67424207bd31e4d52ea175f21584ee72636e87bf1f72a394a9cd1295cdd802752d6d588d07c21030080a96c3b
SSDEEP:	6144:B1PHYG9KkdhRgyGzlYFVXzHlQnOhiyWTKF2DiWAjMTqvFSTixno2EfMkhB5FYB:nYyvd3aY7GOcy9oidjMutJ6+SB56
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r.fa.....0..V.....u... .....@.. .....@.....@.....

File Icon

Icon Hash:	c4b28ed696aa92c0

Static PE Info

General

Entrypoint:	0x46759e
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:	0x6166A672 [Wed Oct 13 09:27:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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	0x655a4	0x65600	False	0.89316093172	data	7.81005656044	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x18cb4	0x18e00	False	0.195420461683	data	5.07149590171	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-08:50:52.634885	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	8.8.8.8	192.168.2.3
10/14/21-08:51:11.745534	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49572	8.8.8.8	192.168.2.3
10/14/21-08:51:30.112821	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57106	8.8.8.8	192.168.2.3
10/14/21-08:51:48.086658	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51539	8.8.8.8	192.168.2.3
10/14/21-08:52:05.282132	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50585	8.8.8.8	192.168.2.3
10/14/21-08:52:22.475142	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58540	8.8.8.8	192.168.2.3
10/14/21-08:52:39.530014	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55108	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 08:50:52.615047932 CEST	192.168.2.3	8.8.8.8	0x4d56	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 08:51:11.725353003 CEST	192.168.2.3	8.8.8.8	0x1eaf	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 14, 2021 08:51:30.092179060 CEST	192.168.2.3	8.8.8.8	0x7d3c	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 14, 2021 08:51:48.066242933 CEST	192.168.2.3	8.8.8.8	0xcfdc	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:05.261580944 CEST	192.168.2.3	8.8.8.8	0x282b	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:22.455004930 CEST	192.168.2.3	8.8.8.8	0x2557	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:39.512092113 CEST	192.168.2.3	8.8.8.8	0x5a6e	Standard query (0)	watermalon 1.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 08:50:52.634885073 CEST	8.8.8.8	192.168.2.3	0x4d56	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:51:11.745533943 CEST	8.8.8.8	192.168.2.3	0x1eaf	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:51:30.112821102 CEST	8.8.8.8	192.168.2.3	0x7d3c	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:51:48.086658001 CEST	8.8.8.8	192.168.2.3	0xcfdc	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:05.282131910 CEST	8.8.8.8	192.168.2.3	0x282b	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:22.475142002 CEST	8.8.8.8	192.168.2.3	0x2557	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)
Oct 14, 2021 08:52:39.530014038 CEST	8.8.8.8	192.168.2.3	0x5a6e	No error (0)	watermalon 1.sytes.net		103.125.189.85	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EDG.exe PID: 2880 Parent PID: 5260

General

Start time:	08:50:38
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\EDG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EDG.exe'
Imagebase:	0x790000
File size:	518144 bytes

MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.297448490.0000000002BA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.297738110.0000000003BA9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.297738110.0000000003BA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.297738110.0000000003BA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: EDG.exe PID: 6208 Parent PID: 2880

General

Start time:	08:50:45
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\EDG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\EDG.exe
Imagebase:	0x8d0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.551341955.0000000006250000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.551341955.0000000006250000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.551341955.0000000006250000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.545032552.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.545032552.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.545032552.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.551181302.00000000061B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.551181302.00000000061B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.549295717.0000000003BC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.549295717.0000000003BC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5528 Parent PID: 6208

General

Start time:	08:50:48
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD97B.tmp'
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1140 Parent PID: 5528

General

Start time:	08:50:49
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6664 Parent PID: 6208

General

Start time:	08:50:50
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDDF0.tmp'
Imagebase:	0x7ff70d6e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3644 Parent PID: 6664

General

Start time:	08:50:50
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: EDG.exe PID: 4848 Parent PID: 664

General

Start time:	08:50:51
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\EDG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\EDG.exe 0
Imagebase:	0x1d0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.320253425.0000000003559000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.320253425.0000000003559000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.320253425.0000000003559000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.319018784.0000000002551000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 1744 Parent PID: 664

General

Start time:	08:50:51
Start date:	14/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x6d0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.323558792.0000000003A09000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.323558792.0000000003A09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.323558792.0000000003A09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.322564022.0000000002A01000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 24%, Virustotal, Browse • Detection: 33%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: EDG.exe PID: 6828 Parent PID: 4848

General

Start time:	08:50:55
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\EDG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\EDG.exe
Imagebase:	0xfe0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.336324291.0000000004619000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.336324291.0000000004619000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.334562407.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.334562407.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.334562407.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.336023952.0000000003611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.336023952.0000000003611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 7060 Parent PID: 1744

General

Start time:	08:50:56
Start date:	14/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xe30000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.340687694.00000000041B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.340687694.00000000041B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.340246832.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.340246832.00000000031B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.337638454.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.337638454.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.337638454.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 3424 Parent PID: 3352

General

Start time:	08:51:01
Start date:	14/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x3f0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.341033995.0000000003729000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.341033995.0000000003729000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.341033995.0000000003729000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.339484800.0000000002721000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 3460 Parent PID: 3424

General

Start time:	08:51:03
Start date:	14/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xf0000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6680 Parent PID: 3424

General

Start time:	08:51:04
Start date:	14/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true

Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x470000
File size:	518144 bytes
MD5 hash:	AD48C92AC820BE7297E6445E9CFEC1C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.355181665.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.355181665.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.355181665.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.356355487.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.356355487.00000000039D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.356262519.00000000029D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.356262519.00000000029D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis