ID: 508706
Sample Name: Debitnote-s3update.exe
Cookbook: default.jbs
Time: 14:44:09
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

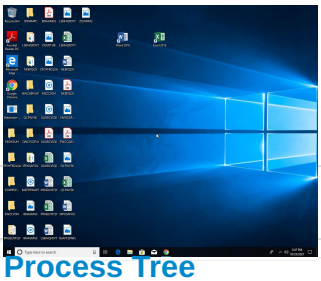
Windows Analysis Report Debitnote-s3update.exe

Overview

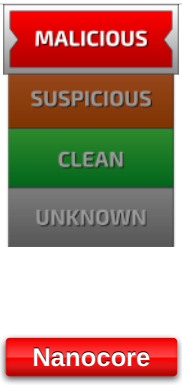
General Information

Sample Name:	Debitnote-s3update.exe
Analysis ID:	508706
MD5:	f162063c8a3c61d..
SHA1:	f8e30f49ca71e8f…
SHA256:	359c0c66cbb2ea…
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



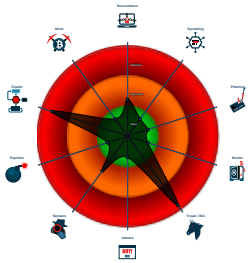
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- 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…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Debitnote-s3update.exe (PID: 6488 cmdline: 'C:\Users\user\Desktop\Debitnote-s3update.exe' MD5: F162063C8A3C61DB87238F88E2E82A81)
  - Debitnote-s3update.exe (PID: 5744 cmdline: C:\Users\user\Desktop\Debitnote-s3update.exe MD5: F162063C8A3C61DB87238F88E2E82A81)
- dhcpmon.exe (PID: 4240 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: F162063C8A3C61DB87238F88E2E82A81)
  - dhcpmon.exe (PID: 3476 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: F162063C8A3C61DB87238F88E2E82A81)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "baa1bd16-ba50-4743-8b51-41c36ee5",
  "Group": "Default",
  "Domain1": "kamuchehddhgfgf.ddns.net",
  "Port": 1187,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "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": "8.8.4.453"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.742502018.0000000002CC1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.742502018.0000000002CC1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x238a7:$a: NanoCore • 0x23900:$a: NanoCore • 0x2393d:$a: NanoCore • 0x239b6:$a: NanoCore • 0x23909:$b: ClientPlugin • 0x23946:$b: ClientPlugin • 0x24244:$b: ClientPlugin • 0x24251:$b: ClientPlugin • 0x1b100:$e: KeepAlive • 0x23d91:$g: LogClientMessage • 0x23d11:$i: get_Connected • 0x158d9:$j: #=q • 0x15909:$j: #=q • 0x15945:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a2d:$j: #=q • 0x15a49:$j: #=q • 0x15a79:$j: #=q
00000000.00000002.689973271.00000000029E2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.740507672.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.740507672.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.dhcpmon.exe.2ce3ac8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
8.2.dhcpmon.exe.2ce3ac8.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
0.2.Debitnote-s3update.exe.3aef648.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Debitnote-s3update.exe.3aef648.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.Debitnote-s3update.exe.3aef648.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 37 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

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

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

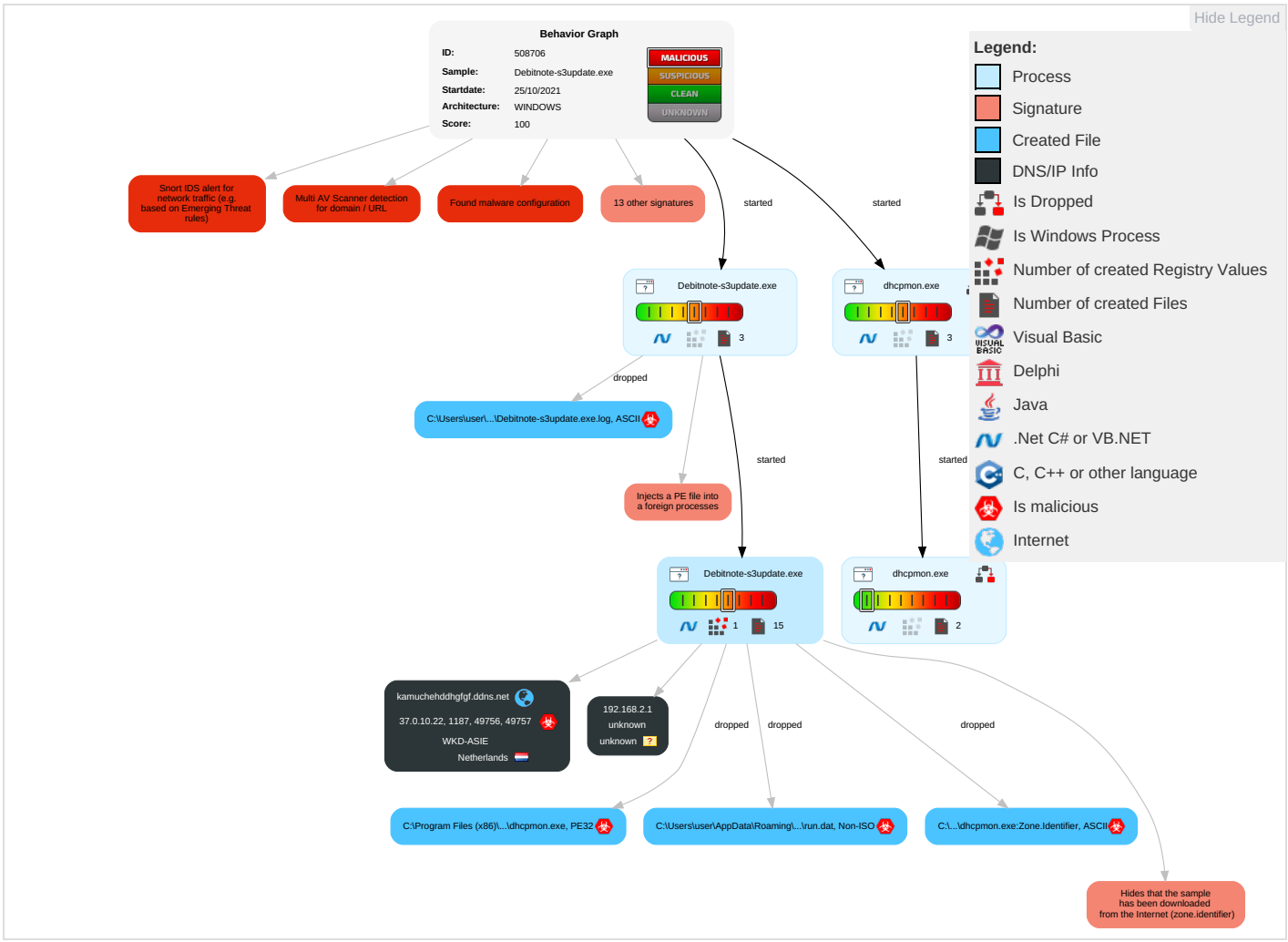
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
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
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 2 1
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
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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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

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
Debitnote-s3update.exe	55%	Virustotal		Browse
Debitnote-s3update.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	
Debitnote-s3update.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
kamuchehddhgfgf.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.carterandcone.comb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
kamuchehddhgfgf.ddns.net	0%	Avira URL Cloud	safe	
http://www.fonts.com)	0%	Avira URL Cloud	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.coma	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.fonts.comicC	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.comyrl	0%	Avira URL Cloud	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	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.carterandcone.comormY	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://en.w0	0%	Avira URL Cloud	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	
http://www.fontbureau.comrsivo	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kamuchehddhgfgf.ddns.net	37.0.10.22	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
kamuchehddhgfgf.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.10.22	kamuchehddhgfgf.ddns.net	Netherlands		198301	WKD-ASIE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508706
Start date:	25.10.2021
Start time:	14:44:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Debitnote-s3update.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:	18
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@6/9@18/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.5%) • Quality average: 21.5% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:45:16	API Interceptor	833x Sleep call for process: Debitnote-s3update.exe modified
14:45:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
14:45:33	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.0.10.22	Purchase Order.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	My CV.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Invoice and waybill.exe	Get hash	malicious	Browse	
	My Resume.exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	
	Balance Payment.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) s.exe	Get hash	malicious	Browse	
	T.T.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kamuchehddhgfgf.ddns.net	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	My CV.exe	Get hash	malicious	Browse	• 37.0.10.22
	Quote.exe	Get hash	malicious	Browse	• 37.0.10.22
	Invoice and waybill.exe	Get hash	malicious	Browse	• 37.0.10.22
	My Resume.exe	Get hash	malicious	Browse	• 37.0.10.22
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	• 37.0.10.22
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	• 37.0.10.22
	Balance Payment.exe	Get hash	malicious	Browse	• 37.0.10.22
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 37.0.10.22
	Circular PSSB Parts Disc Credit Term (Dlr) s.exe	Get hash	malicious	Browse	• 37.0.10.22
	T.T.exe	Get hash	malicious	Browse	• 37.0.10.22

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WKD-ASIE	SKypfeGItc.exe	Get hash	malicious	Browse	• 37.0.10.190
	Purchase Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	HBC.exe	Get hash	malicious	Browse	• 37.0.10.15
	85QKQNr7mm.xlsx	Get hash	malicious	Browse	• 37.0.10.15
	AB948F038175411DC326A1AAD83DF48D6B656325 01551.exe	Get hash	malicious	Browse	• 37.0.8.235
	FC2E04D392AB5E508FDF6C90CE456BFD0AF6DEF1 F10A2.exe	Get hash	malicious	Browse	• 37.0.10.214
	3qZB2fO4lG.exe	Get hash	malicious	Browse	• 37.0.8.193
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86 F0E3E.exe	Get hash	malicious	Browse	• 37.0.11.8
	CQUOTATION REQUEST4.scr.exe	Get hash	malicious	Browse	• 37.0.10.252
	gy6JsH7kJx.exe	Get hash	malicious	Browse	• 37.0.10.225
	About company.doc	Get hash	malicious	Browse	• 37.0.10.225
	SecuriteInfo.com.Virus.Win32.Save.a.26327.exe	Get hash	malicious	Browse	• 37.0.10.225
	ifCgoV9Ykq.exe	Get hash	malicious	Browse	• 37.0.10.225
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	download.dat.exe	Get hash	malicious	Browse	• 37.0.10.13
	TA9015--AA-TA9015-000786-AA-TA9015--AA-TA9015.exe	Get hash	malicious	Browse	• 37.0.10.13
	My CV.exe	Get hash	malicious	Browse	• 37.0.10.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	701952
Entropy (8bit):	7.859478577304115
Encrypted:	false
SSDEEP:	12288:jTq9Ad4zNrL8AuoWBaPXcP9p5YuD1E4qgPJc5e+vzvUxIXN/rN:jTwAGjuoWQclbDDmSmz1/rN
MD5:	F162063C8A3C61DB87238F88E2E82A81
SHA1:	F8E30F49CA71E8F733774C5BD0F770659BDB93FF
SHA-256:	359C0C66CBB2EABF2771A62A2A87762734B73457CF431D1A7E0C94E3A4AB3CFA
SHA-512:	C3BCDFC4BFBE63D3A0B1A0CAD7A21C28DE7948E8C5571DFCE21045E2849F1AED931F3DF504B8C3ADC0ED3D6A1775754FC939B5FA3DA752C56D9843F2EED20B3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....|sa.....0.....Z.... .....@.. ....@.....O..... ....H.....text...`.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....<.....H.....lV...A.....a.....2.....0..@.....+...o.....(.....(.....X...o....2.(..... ....(....*.0.....~.....eo.....+..*...0.... .....~.....o.....+..*.s.....*...0..j.....(.....(.....{.....,..(.....(.....(.....(.....(.....(.....{....o.....1.(.....+....-..(....*...0.....{.....9....r...p(.....+~...+i..{.....(....o|.....,J..{.....(....o|...r...p..o....o.....o.....<.....o.....<

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Debitnote-s3update.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_v2.0_32\UsageLogs\Debitnote-s3update.exe.log	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_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):	525

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.117516745217376
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7V9NhyleajI0fuONKcpMe5i:X4LEnybgCFCtvd7V9NYRj+GONKaMv
MD5:	CF55DF705B79F961ED069D8E84D2AF1C
SHA1:	574CDF36753CF356A25872BCCAA3CC6FFCD5D23F
SHA-256:	DF982E10764D21FCB1469EB6EA1175AC69544C68900B0DD8C79A0FE8A8F300F5
SHA-512:	518A037DF1D6FBC8A296DA5B96B67E073FB1F674090AFE3243E52A65B169DE35FC041C2C05F7EEF9EC74A0100A422E53B3D7D920E5ADF6CE42B82FE94244F5E
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL...Q.F...@.h.....y.[....e..<..n....B...PP...azZ).~..Uj.>..H.b.O..AX.E.S&.O.k.3O'.Lge...$..teI....Hw.CT.].Z.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Debitnote-s3update.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:xt:r
MD5:	86C3FD2DF4F077CE7DF626236871A2DA
SHA1:	A9D806CBB32A48C33A9952C8737053AB812FB001
SHA-256:	62963D728467DC5A4EB9939347CD3AD8DD33CE67DAF2FCC717F6CEDC98275422
SHA-512:	8F6F3003C597DA58E3886A4226F4004D17FC793B8101C4835D6889F456FAC85DACE8DCF2D6231ECD2CCF75E66C2C4B8E51207852041B29996016AD47BB6037B
Malicious:	**true**
Preview:	.6.L...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Debitnote-s3update.exe
File Type:	data
Category:	dropped
Size (bytes):	412824
Entropy (8bit):	**7.999596596836973**
Encrypted:	**true**
SSDEEP:	12288:8l9gnTsbHFPV7iGQVIB8XBLeMb2qLB1rRxH:8QbHFxB8gMiQRxH
MD5:	C9DF8F232494E30402189920360F0907
SHA1:	F181CE82F56D624408AFD68FE82A6A9D77A23383
SHA-256:	ADA0DF11313089119C94406A8EF300442BC1F42ACFA44DF840F5FA9C732026C3
SHA-512:	541579149843E1C08AEAA60DCC5C379D74D87BD7538B6E84D6476E79A65324BB023DFEE5E44F8BF1E794B94F83E5902FE84F4722CFEED37B1C426B97F4F4376
Malicious:	false
Preview:	FF)d6...0...{..X$.E.v>..'9}G>W.S.K.....(..">b/(..m...d....G1.Fwf..1jr..2.i.K}..,.W....;;..y..U.b.O...1.kb...u...4.]7...D.W..Ci..k.U..+...%..D.[.W..6/.....j...w..4p...w...e...v..E...CV'.<... .YN.....t2.....p.k..6..[...N.I...Dg..L....O>.H...^..8Kifc....%...yX....e.....y.-O...%.....m_..v..5.A.3.8...A.;.|.3p .yf('..Z.2Sv...Q.&.4...80.h....7u.a..~[....zr.V:cP:f..cy.f....F.b@.... ....Hu.fs.....b...l.V..u...p.p.h.S..'...*?.....5.JMa.....s,.<k.bo.V.)<.[R.-.....myP._Y.$...#dS....XN..IE.....Q..w.s`.....<.t.....`.T<.....C.....<..e.....p&...F..{. ,nA..".m..$.H D`.:..g.....8...P@/PCxU8>{.....1|_fX.....t.:.....X.\..<..._....7u...2.S2Rx...'../.4..0:P...i....DY..].....R....)..0F...M..w..f.....EV.T...v.r..D.K..Yuz \.K+.....y.`...<.!.C...R...C.. s:)..=vL..$}6..1...?A(DJ.....t..u..xg{.C$8..k.P0..f..D8..g.b..'es....pX..q..[..@32u..1.`.hy.B.*;.c.....w.....o...Z.s.d.$.j..!%v..2....{..P...CP.I.X...}w."\.\-

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.859478577304115
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:	Debitnote-s3update.exe
File size:	701952
MD5:	f162063c8a3c61db87238f88e2e82a81
SHA1:	f8e30f49ca71e8f733774c5bd0f770659bdb93ff
SHA256:	359c0c66cbb2eabf2771a62a2a87762734b73457cf431d1a7e0c94e3a4ab3cfa
SHA512:	c3bcdfc4bfbe63d3a0b1a0cad7a21c28de7948e8c5571dfce21045e2849f1aed931f3df504b8c3adc0ed3d6a1775754fc939b5fa3da752c56d9843f2eed250b3
SSDEEP:	12288:jTq9Ad4zNrL8AuoWBaPXcP9p5YuD1E4qgPJc5e+vzvUxIXN/rN:jTwAGjuoWQclbDDmSmz1/rN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....|sa.....0.....Z.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4aca5a
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:	0x61737CEC [Sat Oct 23 03:09:32 2021 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	0xaaa60	0xaac00	False	0.921517546669	data	7.86674743084	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x5c4	0x600	False	0.425130208333	data	4.13412205535	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	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
10/25/21-14:45:21.664385	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	1187	192.168.2.4	37.0.10.22
10/25/21-14:45:30.784967	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.8.8	192.168.2.4
10/25/21-14:45:31.352807	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	1187	192.168.2.4	37.0.10.22
10/25/21-14:45:41.180533	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	1187	192.168.2.4	37.0.10.22
10/25/21-14:45:50.656891	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	1187	192.168.2.4	37.0.10.22
10/25/21-14:45:55.600682	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49910	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/25/21-14:45:55.629398	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:02.293198	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:09.479824	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:16.510060	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:22.739974	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:28.850927	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:34.703543	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49612	8.8.8.8	192.168.2.4
10/25/21-14:46:34.731419	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:40.633489	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:46.665479	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50601	8.8.8.8	192.168.2.4
10/25/21-14:46:46.755587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:52.749851	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	1187	192.168.2.4	37.0.10.22
10/25/21-14:46:58.651503	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4
10/25/21-14:46:58.683393	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49838	1187	192.168.2.4	37.0.10.22
10/25/21-14:47:03.073219	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	1187	192.168.2.4	37.0.10.22
10/25/21-14:47:08.996250	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	1187	192.168.2.4	37.0.10.22
10/25/21-14:47:14.911234	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	1187	192.168.2.4	37.0.10.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 14:45:21.562231064 CEST	192.168.2.4	8.8.8.8	0x408c	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:30.758384943 CEST	192.168.2.4	8.8.8.8	0xd556	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:41.073146105 CEST	192.168.2.4	8.8.8.8	0xa92d	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:50.592943907 CEST	192.168.2.4	8.8.8.8	0x2edc	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:55.578753948 CEST	192.168.2.4	8.8.8.8	0x4e53	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:02.245498896 CEST	192.168.2.4	8.8.8.8	0x3e61	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:09.162899017 CEST	192.168.2.4	8.8.8.8	0x646b	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:16.462050915 CEST	192.168.2.4	8.8.8.8	0x27e5	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:22.683264971 CEST	192.168.2.4	8.8.8.8	0x53a1	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:28.797502995 CEST	192.168.2.4	8.8.8.8	0xa00	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:34.683144093 CEST	192.168.2.4	8.8.8.8	0x9ce5	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:40.586491108 CEST	192.168.2.4	8.8.8.8	0x1c28	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 14:46:46.644082069 CEST	192.168.2.4	8.8.8.8	0x1ad7	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:52.701982975 CEST	192.168.2.4	8.8.8.8	0xa1ad	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:58.631474972 CEST	192.168.2.4	8.8.8.8	0xcad7	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:03.028523922 CEST	192.168.2.4	8.8.8.8	0x9b42	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:08.946435928 CEST	192.168.2.4	8.8.8.8	0x9a99	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:14.855684996 CEST	192.168.2.4	8.8.8.8	0x2229	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 14:45:21.582407951 CEST	8.8.8.8	192.168.2.4	0x408c	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:30.784966946 CEST	8.8.8.8	192.168.2.4	0xd556	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:41.091525078 CEST	8.8.8.8	192.168.2.4	0xa92d	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:50.611149073 CEST	8.8.8.8	192.168.2.4	0x2edc	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:45:55.600682020 CEST	8.8.8.8	192.168.2.4	0x4e53	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:02.264076948 CEST	8.8.8.8	192.168.2.4	0x3e61	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:09.185523987 CEST	8.8.8.8	192.168.2.4	0x646b	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:16.480628967 CEST	8.8.8.8	192.168.2.4	0x27e5	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:22.701802969 CEST	8.8.8.8	192.168.2.4	0x53a1	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:28.815942049 CEST	8.8.8.8	192.168.2.4	0xa00	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:34.703542948 CEST	8.8.8.8	192.168.2.4	0x9ce5	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:40.604971886 CEST	8.8.8.8	192.168.2.4	0x1c28	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:46.665478945 CEST	8.8.8.8	192.168.2.4	0x1ad7	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:52.718069077 CEST	8.8.8.8	192.168.2.4	0xa1ad	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:46:58.651503086 CEST	8.8.8.8	192.168.2.4	0xcad7	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:03.044851065 CEST	8.8.8.8	192.168.2.4	0x9b42	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:08.964937925 CEST	8.8.8.8	192.168.2.4	0x9a99	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 14:47:14.874916077 CEST	8.8.8.8	192.168.2.4	0x2229	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Debitnote-s3update.exe PID: 6488 Parent PID: 1368

General

Start time:	14:45:09
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\Debitnote-s3update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Debitnote-s3update.exe'
Imagebase:	0x2b0000
File size:	701952 bytes
MD5 hash:	F162063C8A3C61DB87238F88E2E82A81
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: 00000000.00000002.689973271.00000000029E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.690361863.00000000039C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.690361863.00000000039C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.690361863.00000000039C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689951422.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Debitnote-s3update.exe PID: 5744 Parent PID: 6488

General

Start time:	14:45:17
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\Debitnote-s3update.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Debitnote-s3update.exe
Imagebase:	0xaf0000

File size:	701952 bytes
MD5 hash:	F162063C8A3C61DB87238F88E2E82A81
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.698767121.0000000004693000.00000004.00000001.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: dhcpmon.exe PID: 4240 Parent PID: 3424

General

Start time:	14:45:31
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x5e0000
File size:	701952 bytes
MD5 hash:	F162063C8A3C61DB87238F88E2E82A81
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: 00000006.00000002.730722572.0000000003D11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.730722572.0000000003D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.730722572.0000000003D11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.728501904.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.728551090.0000000002D32000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 58%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 3476 Parent PID: 4240

General

Start time:	14:45:34
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x540000
File size:	701952 bytes
MD5 hash:	F162063C8A3C61DB87238F88E2E82A81
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: 00000008.00000002.742502018.0000000002CC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.742502018.0000000002CC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.740507672.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.740507672.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.740507672.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.742614209.0000000003CC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.742614209.0000000003CC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis