



ID: 402865
Sample Name: note-mxm.exe
Cookbook: default.jbs
Time: 15:06:57
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report note-mxm.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16

Copyright Joe Security LLC 2021

Entrypoint Preview 17
Data Directories 18
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Snort IDS Alerts 19
TCP Packets 20
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: note-mxm.exe PID: 6860 Parent PID: 5944 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 25
Analysis Process: schtasks.exe PID: 7064 Parent PID: 6860 25
General 25
File Activities 26
File Read 26
Analysis Process: conhost.exe PID: 7072 Parent PID: 7064 26
General 26
Analysis Process: note-mxm.exe PID: 7120 Parent PID: 6860 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
File Read 28
Disassembly 29
Code Analysis 29

Copyright Joe Security LLC 2021

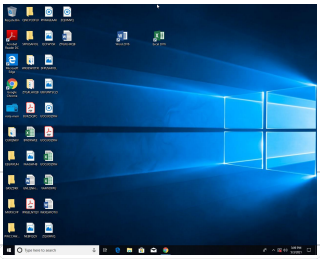
Analysis Report note-mxm.exe

Overview

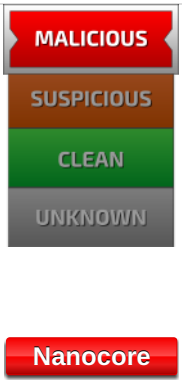
General Information

Sample Name:	note-mxm.exe
Analysis ID:	402865
MD5:	116db2200d9be3..
SHA1:	29cf6588682aca6..
SHA256:	43bc7ada656332..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

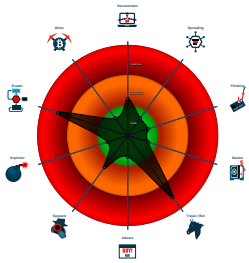


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- note-mxm.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\note-mxm.exe' MD5: 116DB2200D9BE33529615FC98907D4D8)
  - schtasks.exe (PID: 7064 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fGAhpbrTQZcHeY' /XML 'C:\Users\user\AppData\Local\Temp\tmp943B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - note-mxm.exe (PID: 7120 cmdline: C:\Users\user\Desktop\note-mxm.exe MD5: 116DB2200D9BE33529615FC98907D4D8)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2.2.0",
  "Mutex": "cbea22e5-f897-4039-a352-cfbfd96f",
  "Group": "chase1",
  "Domain1": "45.137.22.50",
  "Domain2": "127.0.0.1",
  "Port": 4557,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x11e25d:$x1: NanoCore.ClientPluginHost • 0x150a7d:$x1: NanoCore.ClientPluginHost • 0x11e29a:$x2: IClientNetworkHost • 0x150aba:$x2: IClientNetworkHost • 0x121dcd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x1545ed:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x11dfc5:$a: NanoCore • 0x11dfd5:$a: NanoCore • 0x11e209:$a: NanoCore • 0x11e21d:$a: NanoCore • 0x11e25d:$a: NanoCore • 0x1507e5:$a: NanoCore • 0x1507f5:$a: NanoCore • 0x150a29:$a: NanoCore • 0x150a3d:$a: NanoCore • 0x150a7d:$a: NanoCore • 0x11e024:$b: ClientPlugin • 0x11e226:$b: ClientPlugin • 0x11e266:$b: ClientPlugin • 0x150844:$b: ClientPlugin • 0x150a46:$b: ClientPlugin • 0x150a86:$b: ClientPlugin • 0x11e14b:$c: ProjectData • 0x15096b:$c: ProjectData • 0x11eb52:$d: DESCrypto • 0x151372:$d: DESCrypto • 0x12651e:$e: KeepAlive
00000000.00000002.670714258.0000000002FBA000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: note-mxm.exe PID: 6860	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
0.2.note-mxm.exe.40870d0.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.note-mxm.exe.40870d0.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x42725:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x429ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x43fe6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x43fda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x44e8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ac42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x429d7:$s5: IClientLoggingHost
0.2.note-mxm.exe.40870d0.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.note-mxm.exe.40870d0.2.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x42715:$a: NanoCore • 0x42725:$a: NanoCore • 0x42959:$a: NanoCore • 0x4296d:$a: NanoCore • 0x429ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x42774:$b: ClientPlugin • 0x42976:$b: ClientPlugin • 0x429b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4289b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x432a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
0.2.note-mxm.exe.40870d0.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Sigma Overview

System Summary:



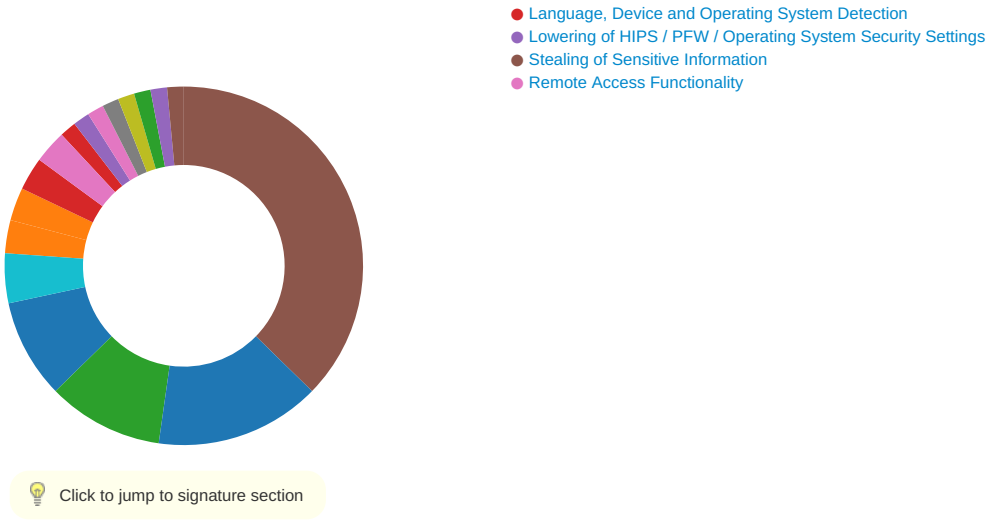
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

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)

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Copyright Joe Security LLC 2021

Remote Access Functionality:



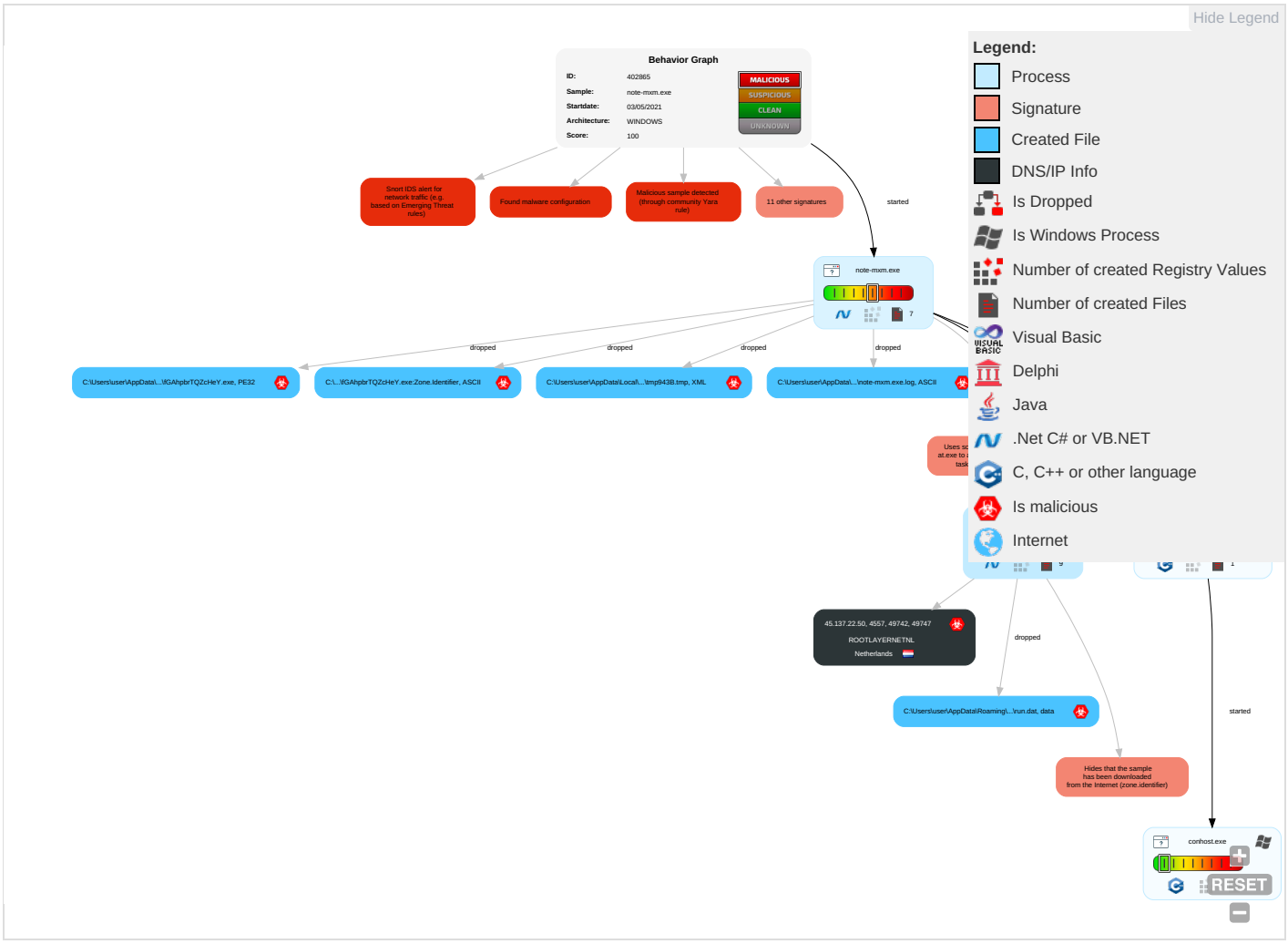
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

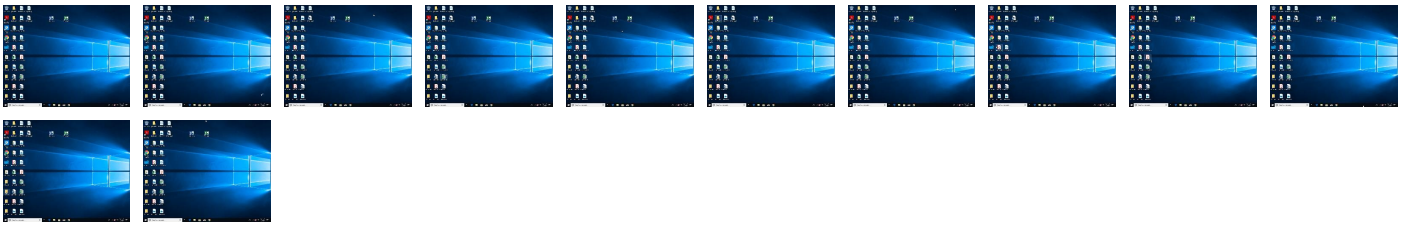
Behavior Graph



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
note-mxm.exe	30%	Metadefender		Browse
note-mxm.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
note-mxm.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	30%	Metadefender		Browse
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
45.137.22.50	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
45.137.22.50	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	note-mxm.exe, 00000000.00000002.670657533.0000000002F71000.00000004.00000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	note-mxm.exe, 00000000.00000002.670714258.0000000002FBA000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.50	unknown	Netherlands		51447	ROOTLAYERNETNL	true

Copyright Joe Security LLC 2021

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402865
Start date:	03.05.2021
Start time:	15:06:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	note-mxm.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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.evad.winEXE@6/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/402865/sample/note-mxm.exe

Simulations

Behavior and APIs

Time	Type	Description
15:07:49	API Interceptor	1037x Sleep call for process: note-mxm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.137.22.50	purchase order confirmation.exe	Get hash	malicious	Browse	
	purchase order acknowledgement.exe	Get hash	malicious	Browse	
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223 DATED 29042021.exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223, date29042021.exe	Get hash	malicious	Browse	
	B_N SAO SWIFT MT103.exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223 DATED 28042021.exe	Get hash	malicious	Browse	
	Al kabous group Ltd - purchase order #04272021.exe	Get hash	malicious	Browse	
	Mack Trading Limited - products list.exe	Get hash	malicious	Browse	
	Kim Quy Trading - PRODUCTS LISTS.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	purchase order confirmation.exe	Get hash	malicious	Browse	• 45.137.22.50
	purchase order acknowledgement.exe	Get hash	malicious	Browse	• 45.137.22.50
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	• 45.137.22.50
	FRIEGHT PAYMENT 41,634.20 USD..exe	Get hash	malicious	Browse	• 45.137.22.107
	Due Invoices.exe	Get hash	malicious	Browse	• 45.137.22.107
	PURCHASE ORDER - #0022223 DATED 29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	PURCHASE ORDER - #0022223, date29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	B_N SAO SWIFT MT103.exe	Get hash	malicious	Browse	• 45.137.22.50
	PO0900009.exe	Get hash	malicious	Browse	• 185.222.58.152
	PURCHASE ORDER - #0022223 DATED 28042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	Order ConfirmationSANQAW12NC9W03.exe	Get hash	malicious	Browse	• 185.222.57.152
	PO MT2249C.exe	Get hash	malicious	Browse	• 185.222.57.152
	Al kabous LtdPurchase order NO#00421876.exe	Get hash	malicious	Browse	• 185.222.57.152
	Al kabous group Ltd - purchase order #04272021.exe	Get hash	malicious	Browse	• 45.137.22.50
	0900000000000000000900.exe	Get hash	malicious	Browse	• 185.222.58.152
	P08240421_CIF-Pdf.exe	Get hash	malicious	Browse	• 45.137.22.123
	ORD-63648.exe	Get hash	malicious	Browse	• 45.137.22.123
	FA0900009000.exe	Get hash	malicious	Browse	• 185.222.58.152
	Packinglist&certificate of imports.exe	Get hash	malicious	Browse	• 185.222.57.152
	TBF-21-52100456221SLIP.exe	Get hash	malicious	Browse	• 185.222.57.152

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	purchase order acknowledgement.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\note-mxm.exe.log

Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\note-mxm.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp943B.tmp	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.190755160932022
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGb0tn:cbhK79lNQR/rydbz9I3YODOLNdq3Ky
MD5:	9C465D88687A175E59A5172F12074D2C
SHA1:	E70078C669274EBEC56EA9BAC13A771C733EA761
SHA-256:	7A090FDE949633CC7492697D753BC20A20967C81CC2FAFDAC5407DA6DF50988C
SHA-512:	A4C718EAB9DBDD6FF0A3896F8E68C71489D44F94A5FD2C7F7191BAB6FB14C5384B1D80EAB6C77850022981A951124FF14F234309B2B06E3FE8E260CCEF1CB291
Malicious:	**true**
Reputation:	low
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>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6B5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:liw:liw
MD5:	7C5B8D5CE01084BCC3DF9F982DBA59F5
SHA1:	E63D0D5F7801A82A6911AA2FF44F4E967A0C7AE6
SHA-256:	11401E31B5922DF5D18F3F361853B328BEE3CB50E5DB7E1151A5532B00417939
SHA-512:	A88E44890F986794EA56B6E4F5BAE44D0E52D2DF0F650FE42ADF343F2F5262845883D49514AAB1D9790568C6FF594BAFB289AAB1C3B7B720DFFF96125D494264
Malicious:	**true**
Reputation:	low
Preview:	-.Mw4..H

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	724480
Entropy (8bit):	7.664537233778505
Encrypted:	false
SSDEEP:	12288:KYaTBJ1qtapo1SuoMwcQvFLJlCLL/HDtysCfO263+LS7EytLMsq9Sv:KYaT/1qt8oM9MK9PCYV6OmEcL9v
MD5:	116DB2200D9BE33529615FC98907D4D8
SHA1:	29CF6588682ACA66C59E41E0517EDE00C75CC76D
SHA-256:	43BC7ADA65633263E408152D7B117DE464C9D23B2758D96A6822BDE9AD27B170
SHA-512:	B4D80A7769365E0975BF03ADD9F59A618E43FA85F12B1A04C40F428FC32BEE65E14EDB4FD38BEB4DD71C5A588762670C0A2CD18452D790289532BE342C5CBFE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 57%
Joe Sandbox View:	• Filename: purchase order acknowledgement.exe, Detection: malicious, Browse

C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....8..... .....@.. .....`..... .@.....\...W.... ..t4..... ....H.....text..... ....`.reloc.....@..B.rsrc...t4... . ..6.....@..@.....H.....^.....7...&.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}... ..*..}..... ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s ...z.2.{.....i..*....0..<.....{.....3.. {....(....o....3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\note-mxm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.664537233778505
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	note-mxm.exe
File size:	724480
MD5:	116db2200d9be33529615fc98907d4d8
SHA1:	29cf6588682aca66c59e41e0517ede00c75cc76d
SHA256:	43bc7ada65633263e408152d7b117de464c9d23b2758d9 6a6822bde9ad27b170
SHA512:	b4d80a7769365e0975bf03add9f59a618e43fa85f12b1a0 4c40f428fc32bee65e14edb4fd38beb4dd71c5a58876267 0c0a2cd18452d790289532be342c5cbf7e
SSDEEP:	12288:KYaTBJ1qtapo1SuoMwcQvFLJlCLL/HDtysCfO2 63+LS7EytLMsq9Sv:KYaT/1qt8oM9MK9PCYV6OmEcL 9v
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .`.....8..... .....@.. .....`..... @.....

File Icon



Icon Hash:	00a275154a880000

Static PE Info

General

Entrypoint:	0x49f3b6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608C93C7 [Fri Apr 30 23:33:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9f35c	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x13474	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9d3bc	0x9d400	False	0.882360703994	data	7.83711506914	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xa0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x13474	0x13600	False	0.20802671371	data	4.32608110804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa2160	0x10828	data		
RT_ICON	0xb2988	0x25b5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb4f40	0x22	data		
RT_VERSION	0xb4f64	0x35c	data		
RT_MANIFEST	0xb52c0	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	SeekOrigin.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	TechSupportRegistration
ProductVersion	1.0.0.0
FileDescription	TechSupportRegistration
OriginalFilename	SeekOrigin.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-15:07:57.124675	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:03.659148	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:10.757124	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:16.850580	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	4557	192.168.2.4	45.137.22.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-15:08:22.830791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:28.864359	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:34.846801	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:40.971003	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:46.397894	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:52.510849	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	4557	192.168.2.4	45.137.22.50
05/03/21-15:08:58.520473	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:04.550871	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:10.601121	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:16.600739	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:22.600482	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:28.606933	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:34.634981	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:40.616698	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:47.945632	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	4557	192.168.2.4	45.137.22.50
05/03/21-15:09:53.914914	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	4557	192.168.2.4	45.137.22.50

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:07:57.037607908 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.084256887 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.084394932 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.124675035 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.196150064 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.221226931 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.270549059 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.285933971 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.362386942 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392587900 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392664909 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392700911 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392734051 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.392741919 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392771959 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.392793894 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.435008049 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.439896107 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.439963102 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.439986944 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.440010071 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440032959 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.440056086 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440057039 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.440102100 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440150023 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440196991 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440226078 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.440244913 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440256119 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.440273046 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.440347910 CEST	49742	4557	192.168.2.4	45.137.22.50

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:07:57.486797094 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.486866951 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.486907005 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.486928940 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487159014 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487211943 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487261057 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487309933 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487324953 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487360954 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487363100 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487411976 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487463951 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487513065 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487565994 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487570047 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487653017 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487680912 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487714052 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487751007 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487776041 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487835884 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487873077 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.487898111 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487946987 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.487951040 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.534754038 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.534823895 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.534883022 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.534931898 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.534956932 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.534981966 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.534998894 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535032988 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535075903 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535084963 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535135031 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535182953 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535234928 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535247087 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535284996 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535295010 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535336018 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535387039 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535393953 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535432100 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535485029 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535486937 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535537004 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535587072 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535605907 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535635948 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535687923 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535712957 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535737991 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535787106 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535808086 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535837889 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535887957 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.535897017 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.535938978 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.536005020 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.536066055 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.536089897 CEST	49742	4557	192.168.2.4	45.137.22.50

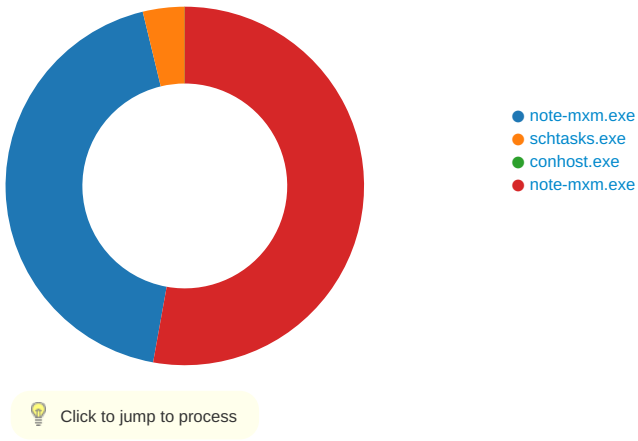
Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:07:57.536144972 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.536176920 CEST	49742	4557	192.168.2.4	45.137.22.50
May 3, 2021 15:07:57.536201954 CEST	4557	49742	45.137.22.50	192.168.2.4
May 3, 2021 15:07:57.536257029 CEST	4557	49742	45.137.22.50	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: note-mxm.exe PID: 6860 Parent PID: 5944

General

Start time:	15:07:47
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\note-mxm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\note-mxm.exe'
Imagebase:	0xbd0000
File size:	724480 bytes
MD5 hash:	116DB2200D9BE33529615FC98907D4D8
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: 00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.671855765.0000000003F79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.670714258.0000000002FBA000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp943B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C227038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\note-mxm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp943B.tmp	success or wait	1	6C226A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fGAhpbrTQZcHeY.exe	0	262144	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 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 c7 93 8c 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d4 09 00 00 38 01 00 00 00 00 00 b6 f3 09 00 00 20 00 00 00 00 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0b 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ...........8........... ........@.. .......................` ....@.................	success or wait	3	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\ fGAhpbrTQZcHeY.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp943B.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\note-mxm.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: schtasks.exe PID: 7064 Parent PID: 6860

General

Start time:	15:07:51
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fGAhpbrTQZcHeY' /XML 'C:\Users\user\AppData\Local\Temp\tmp943B.tmp'
Imagebase:	0x980000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Copyright Joe Security LLC 2021

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp943B.tmp	unknown	2	success or wait	1	98AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp943B.tmp	unknown	1648	success or wait	1	98ABD9	ReadFile

Analysis Process: conhost.exe PID: 7072 Parent PID: 7064

General

Start time:	15:07:51
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: note-mxm.exe PID: 7120 Parent PID: 6860

General

Start time:	15:07:52
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\note-mxm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\note-mxm.exe
Imagebase:	0xe50000
File size:	724480 bytes
MD5 hash:	116DB2200D9BE33529615FC98907D4D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	17	6C221E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\note-mxm.exe:Zone.Identifier	success or wait	1	6C1A2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	2d a0 4d 77 34 0e d9 48	-.Mw4..H	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	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.....&.	success or wait	8	6C221B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .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.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C221B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\Desktop\note-mxm.exe	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Users\user\Desktop\note-mxm.exe	unknown	512	success or wait	1	6D39D72F	unknown

Disassembly

Code Analysis