ID: 433265
Sample Name: OMANTECH PRODUCTS.exe
Cookbook: default.jbs
Time: 14:59:16
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

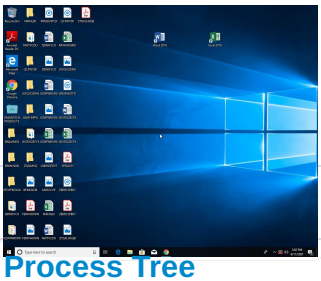
Analysis Report OMANTECH PRODUCTS.exe

Overview

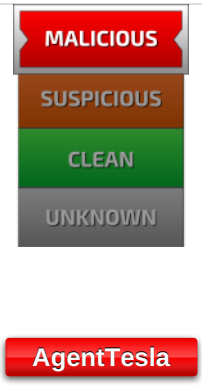
General Information

Sample Name:	OMANTECH PRODUCTS.exe
Analysis ID:	433265
MD5:	1603b2e2474ac5..
SHA1:	a50dbd334f5d9a6.
SHA256:	1e718cc81b1725..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



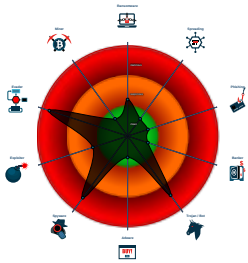
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- OMANTECH PRODUCTS.exe (PID: 6696 cmdline: 'C:\Users\user\Desktop\OMANTECH PRODUCTS.exe' MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
  - OMANTECH PRODUCTS.exe (PID: 6844 cmdline: C:\Users\user\Desktop\OMANTECH PRODUCTS.exe MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
- EupFNx.exe (PID: 6336 cmdline: 'C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe' MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
  - EupFNx.exe (PID: 6488 cmdline: C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
- EupFNx.exe (PID: 6568 cmdline: 'C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe' MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
  - EupFNx.exe (PID: 5916 cmdline: C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
  - EupFNx.exe (PID: 5808 cmdline: C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe MD5: 1603B2E2474AC57BA3EE0AE98357B50C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "jokelogs@omnlltd.comE#@Dfb$LbM)Mserver126.web-hosting.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000000.438386722.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000000.438386722.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.582625158.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.582625158.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.446184699.00000000030F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 33 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.EupFNx.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
17.2.EupFNx.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.OMANTECH PRODUCTS.exe.3ba3e38.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.OMANTECH PRODUCTS.exe.3ba3e38.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.EupFNx.exe.4573e38.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

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

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

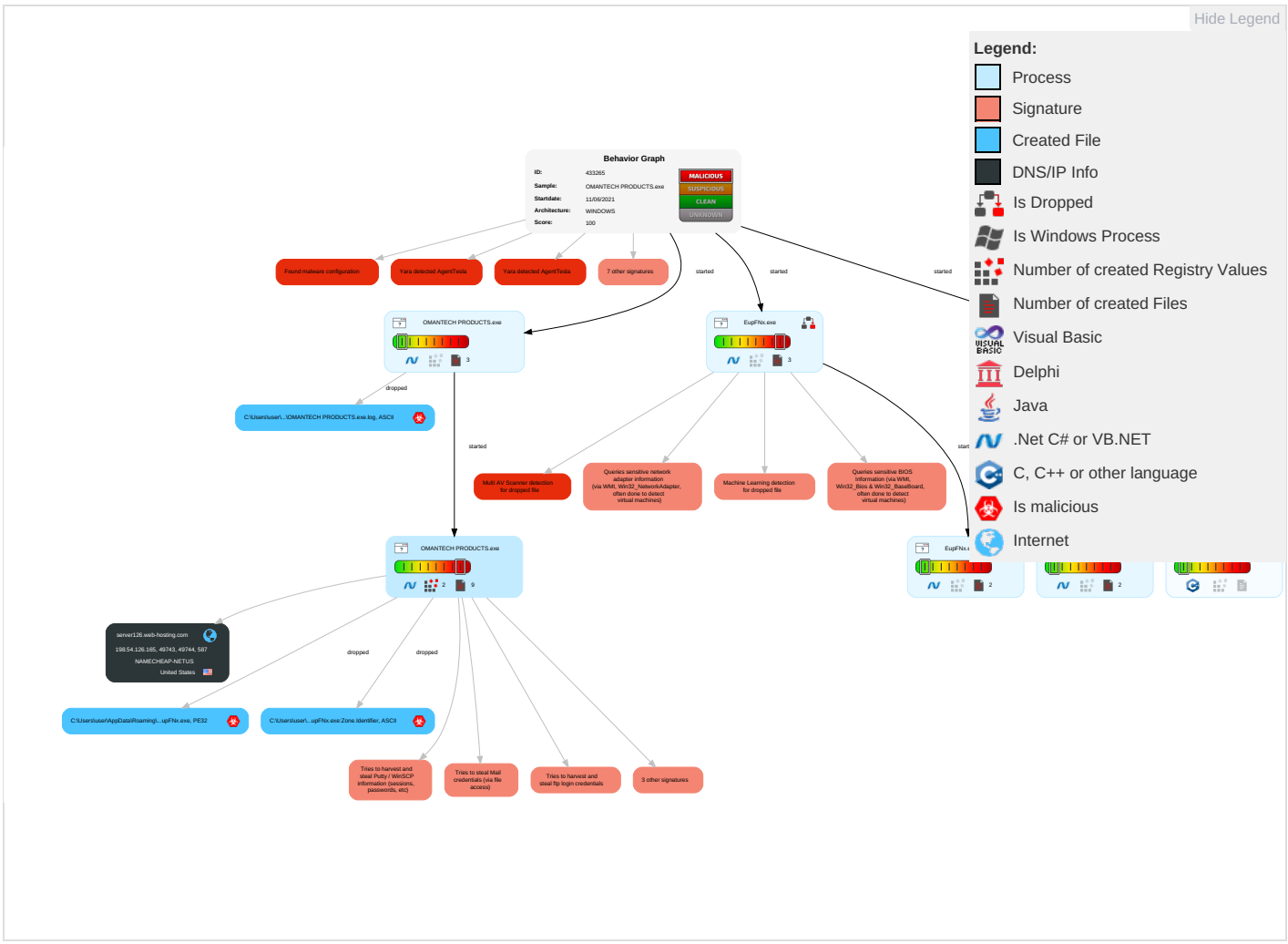
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypt Channe
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-St Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr

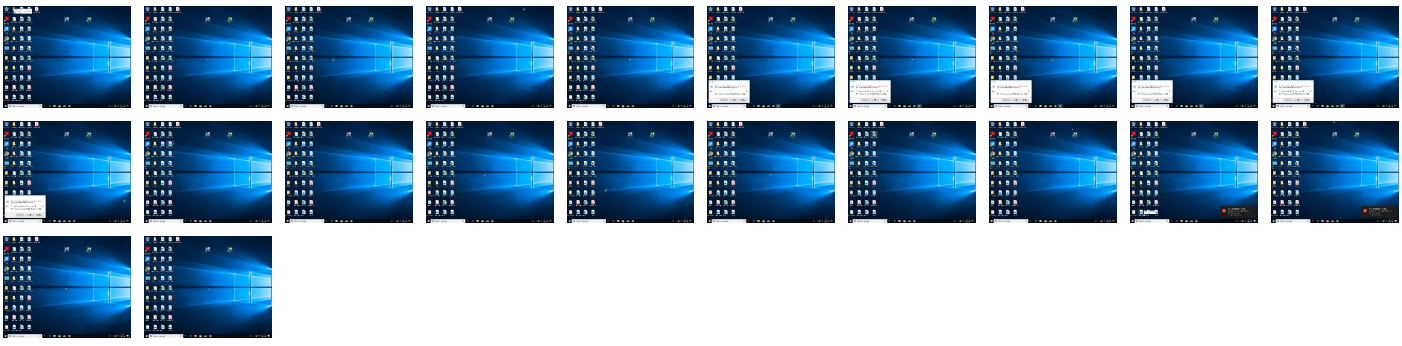
Behavior Graph



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
OMANTECH PRODUCTS.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.OMANTECH PRODUCTS.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.2.EupFNx.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.OMANTECH PRODUCTS.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.0.EupFNx.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.EupFNx.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.EupFNx.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ronNgX.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0-	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://sAxmBjuRp77zUAl6sU9.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
server126.web-hosting.com	198.54.126.165	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.126.165	server126.web-hosting.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433265
Start date:	11.06.2021
Start time:	14:59:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 19s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OMANTECH PRODUCTS.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:	25
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.spyw.evad.winEXE@11/5@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.4%) • Quality average: 38.1% • Quality standard deviation: 43.9%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:00:03	API Interceptor	759x Sleep call for process: OMANTECH PRODUCTS.exe modified
15:00:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run EupFNx C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
15:00:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run EupFNx C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
15:00:43	API Interceptor	338x Sleep call for process: EupFNx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.126.165	TWO NEW QUOTATION.exe	Get hash	malicious	Browse	
	GOE2103001 SHPT.exe	Get hash	malicious	Browse	
	VVw0lC8P5l.exe	Get hash	malicious	Browse	
	14776260521.pdf.exe	Get hash	malicious	Browse	
	PO_20211153 Dt-241.exe	Get hash	malicious	Browse	
	INV-257591_77134027.pdf.exe	Get hash	malicious	Browse	
	PO 100251 05202021.exe	Get hash	malicious	Browse	
	7b1371c7_by_Libranalysis.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	specifications.exe	Get hash	malicious	Browse	
	cargo details.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Import shipment.exe	Get hash	malicious	Browse	
	PROJECT SPECIFICATION.exe	Get hash	malicious	Browse	
	customer request.exe	Get hash	malicious	Browse	
	Import shipment.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	MV BBG WUZHOU.exe	Get hash	malicious	Browse	
	products & catalog.exe	Get hash	malicious	Browse	
	Bunker Form 1.exe	Get hash	malicious	Browse	
	new purchase order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
server126.web-hosting.com	TWO NEW QUOTATION.exe	Get hash	malicious	Browse	• 198.54.126.165
	GOE2103001 SHPT.exe	Get hash	malicious	Browse	• 198.54.126.165
	VVw0lC8P5l.exe	Get hash	malicious	Browse	• 198.54.126.165
	14776260521.pdf.exe	Get hash	malicious	Browse	• 198.54.126.165
	PO_20211153 Dt-241.exe	Get hash	malicious	Browse	• 198.54.126.165
	INV-257591_77134027.pdf.exe	Get hash	malicious	Browse	• 198.54.126.165
	PO 100251 05202021.exe	Get hash	malicious	Browse	• 198.54.126.165
	7b1371c7_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.126.165
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	specifications.exe	Get hash	malicious	Browse	• 198.54.126.165
	cargo details.exe	Get hash	malicious	Browse	• 198.54.126.165
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	PROJECT SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.126.165
	customer request.exe	Get hash	malicious	Browse	• 198.54.126.165
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.126.165
	MV BBG WUZHOU.exe	Get hash	malicious	Browse	• 198.54.126.165
	products & catalog.exe	Get hash	malicious	Browse	• 198.54.126.165
	Bunker Form 1.exe	Get hash	malicious	Browse	• 198.54.126.165
	new purchase order.exe	Get hash	malicious	Browse	• 198.54.126.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	main_setup_x86x64.exe	Get hash	malicious	Browse	• 198.54.116.159
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 198.54.116.159
	w4X8dxtGi6.exe	Get hash	malicious	Browse	• 198.54.116.159
	c71fd2gJus.exe	Get hash	malicious	Browse	• 198.54.116.159
	BrBsL8sBvm.exe	Get hash	malicious	Browse	• 198.54.116.159
	bL6FwQU4K5.exe	Get hash	malicious	Browse	• 198.54.126.101
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 198.54.116.159
	crt9O3URua.exe	Get hash	malicious	Browse	• 198.54.116.159
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 198.54.116.159
	3JDjILxXaA.exe	Get hash	malicious	Browse	• 198.54.116.159
	SecuriteInfo.com.Heur.23766.xls	Get hash	malicious	Browse	• 68.65.122.53
	#Ud83d#Udce9-peter.nash.htm	Get hash	malicious	Browse	• 185.61.154.34
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 198.54.117.216
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 162.0.229.108
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 68.65.122.148
	3arZKnr21W.exe	Get hash	malicious	Browse	• 198.54.116.180
	hdOkhI5TaNNo08q.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO187439.exe	Get hash	malicious	Browse	• 198.54.117.217
	Nr_0052801.exe	Get hash	malicious	Browse	• 198.54.122.60
	YI6482CO6U.exe	Get hash	malicious	Browse	• 198.54.126.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EupFNx.exe.log	
Process:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
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\Microsoft\CLR_v4.0_32\UsageLogs\OMANTECH PRODUCTS.exe.log	
Process:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
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\Roaming\EupFNx\EupFNx.exe	
Process:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	958464
Entropy (8bit):	7.51111975155998
Encrypted:	false
SSDEEP:	24576:0UlxWPIid63/m5+tSH0exuIwBB+NeBUdt:luPtf5600EuI4+wBU
MD5:	1603B2E2474AC57BA3EE0AE98357B50C
SHA1:	A50DBD334F5D9A67C51B399DFC9C8B44B5514E59
SHA-256:	1E718CC81B172505BAB7576339BB954E9911C79C95C67430355AFC493D075A2E
SHA-512:	40FE6DC78C4CBA912E7BDAB62B50D74B70B5247855A4B0C3282361F73717FFCACA986226B5EF02A8AA79F691E1FA379CAD0F7FB8518EF8D9807A2F35CE1D605C
Malicious:	**true**

C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R..`..... ... ....@.. ..... ..... ..@.....K....@.....?..... ..... ..H.....text..... ..... ..`.sdata..... .....@....rsr c.....@.....@..@.reloc.....@..B..... ....

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

C:\Users\user\AppData\Roaming\a0rwr13c.dji\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.51111975155998
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	OMANTECH PRODUCTS.exe
File size:	958464
MD5:	1603b2e2474ac57ba3ee0ae98357b50c
SHA1:	a50dbd334f5d9a67c51b399dfc9c8b44b5514e59

General

SHA256:	1e718cc81b172505bab7576339bb954e9911c79c95c67430355afc493d075a2e
SHA512:	40fe6dc78c4cba912e7bdab62b50d74b70b5247855a4b0c3282361f73717ffcaca986226b5ef02a8aa79f691e1fa379cad0f7fb8518ef8d9807a2f35ce1d609c
SSDEEP:	24576:0UlxWPIid63/m5+tSH0exuIwBB+NeBUdt:luPtf5600EuI4+wBU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R..`..... ... .@.. ....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x4c12de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
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:	0x60C2A252 [Thu Jun 10 23:37:54 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbf2e4	0xbf400	False	0.896582669526	data	7.85494493931	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc2000	0x1e8	0x200	False	0.861328125	data	6.63158586032	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x2a388	0x2a400	False	0.12430658284	data	4.17143589292	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:01:54.840763092 CEST	192.168.2.6	8.8.8.8	0xae1	Standard query (0)	server126.web-hosting.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:02:02.612732887 CEST	192.168.2.6	8.8.8.8	0x520d	Standard query (0)	server126.web-hosting.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:01:54.919526100 CEST	8.8.8.8	192.168.2.6	0xae1	No error (0)	server126.web-hosting.com		198.54.126.165	A (IP address)	IN (0x0001)
Jun 11, 2021 15:02:02.674289942 CEST	8.8.8.8	192.168.2.6	0x520d	No error (0)	server126.web-hosting.com		198.54.126.165	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 15:01:55.677628040 CEST	587	49743	198.54.126.165	192.168.2.6	220-server126.web-hosting.com ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 09:01:55 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 15:01:55.678328037 CEST	49743	587	192.168.2.6	198.54.126.165	EHLO 019635
Jun 11, 2021 15:01:55.875596046 CEST	587	49743	198.54.126.165	192.168.2.6	250-server126.web-hosting.com Hello 019635 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 15:01:55.876219988 CEST	49743	587	192.168.2.6	198.54.126.165	STARTTLS
Jun 11, 2021 15:01:56.075303078 CEST	587	49743	198.54.126.165	192.168.2.6	220 TLS go ahead
Jun 11, 2021 15:02:03.130382061 CEST	587	49744	198.54.126.165	192.168.2.6	220-server126.web-hosting.com ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 09:02:03 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 15:02:03.130775928 CEST	49744	587	192.168.2.6	198.54.126.165	EHLO 019635
Jun 11, 2021 15:02:03.325664043 CEST	587	49744	198.54.126.165	192.168.2.6	250-server126.web-hosting.com Hello 019635 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 11, 2021 15:02:03.326008081 CEST	49744	587	192.168.2.6	198.54.126.165	STARTTLS
Jun 11, 2021 15:02:03.524975061 CEST	587	49744	198.54.126.165	192.168.2.6	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: OMANTECH PRODUCTS.exe PID: 6696 Parent PID: 5936

General

Start time:	15:00:01
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OMANTECH PRODUCTS.exe'
Imagebase:	0x6c0000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.328789854.0000000003AE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.328789854.0000000003AE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.328280994.0000000002B1F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: OMANTECH PRODUCTS.exe PID: 6844 Parent PID: 6696

General

Start time:	15:00:04
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OMANTECH PRODUCTS.exe
Imagebase:	0xf50000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.582625158.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.582625158.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.324134931.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.324134931.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.591441667.0000000003301000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: EupFNx.exe PID: 6336 Parent PID: 3440

General

Start time:	15:00:41
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe'
Imagebase:	0xed0000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
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: 00000007.00000002.414812031.00000000034EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.415888638.00000000044B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.415888638.00000000044B9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: EupFNx.exe PID: 6488 Parent PID: 6336

General

Start time:	15:00:45
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Imagebase:	0xd60000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.446184699.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.446184699.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.411469581.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.411469581.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.443402056.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.443402056.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: EupFNx.exe PID: 6568 Parent PID: 3440

General

Start time:	15:00:49
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe'
Imagebase:	0x570000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.443519142.00000000039F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.443519142.00000000039F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.442857843.0000000002A2F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: EupFNx.exe PID: 5916 Parent PID: 6568

General

Start time:	15:00:55
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Imagebase:	0x3b0000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: EupFNx.exe PID: 5808 Parent PID: 6568

General

Start time:	15:00:57
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\EupFNx\EupFNx.exe
Imagebase:	0x440000
File size:	958464 bytes
MD5 hash:	1603B2E2474AC57BA3EE0AE98357B50C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.438386722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.438386722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.590870590.00000000027C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.590870590.00000000027C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.582257819.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.582257819.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis