ID: 442547
Sample Name:
policy#37820.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:05:00
Date: 30/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

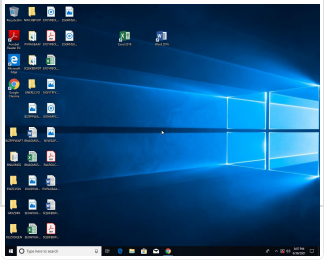
Windows Analysis Report policy#37820.xlsb

Overview

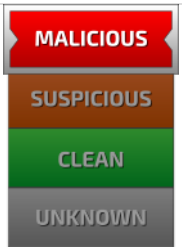
General Information

Sample Name:	policy#37820.xlsb
Analysis ID:	442547
MD5:	f60146ee4fab89e..
SHA1:	82bb4929a849de..
SHA256:	6ab90a34f6fdfaf1..
Infos:	

Most interesting Screenshot:



Detection



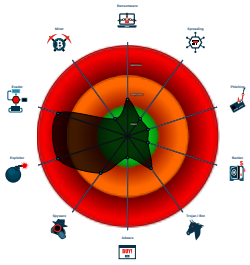
RMSRemoteAdmin Hidden Macro 4.0

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Office document tries to convince vi…
- Contains functionality to create proc…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found abnormal large hidden Excel …
- Office process drops PE file
- Query firmware table information (lik…
- Sigma detected: Execution from Sus…
- Sigma detected: Microsoft Office Pr…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5412 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 6388 cmdline: wmic process call create 'C:\Users\Public\Libraries/appscomhost' MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- appscomhost (PID: 6596 cmdline: C:\Users\Public\Libraries/appscomhost MD5: 8DF649FAB065908962626C67F247618C)
  - Javelin.exe (PID: 6832 cmdline: 'C:\Users\Public\JavelinNew\Javelin.exe' MD5: AF5879D56594F01794A2C028BC75EC27)
    - Javelin.exe (PID: 7128 cmdline: C:\Users\Public\JavelinNew\Javelin.exe -run_agent -second MD5: AF5879D56594F01794A2C028BC75EC27)
      - cmd.exe (PID: 6308 cmdline: C:\Windows\system32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - net.exe (PID: 6836 cmdline: net user /domain MD5: DD0561156F62BC1958CE0E370B23711B)
          - net1.exe (PID: 6436 cmdline: C:\Windows\system32\net1 user /domain MD5: B5A26C2BF17222E86B91D26F1247AF3E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\JavelinNew\Javelin.exe	JoeSecurity_RMSRemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
C:\Users\Public\JavelinNew\Javelin.exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.300472994.000000000120 8000.00000002.00020000.sdmp	JoeSecurity_RMSRemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.273261388.000000000120 8000.00000002.00020000.sdmp	JoeSecurity_RMSRemote Admin	Yara detected RMS RemoteAdmin tool	Joe Security	
0000000B.00000003.311749860.000000007D91 0000.00000004.00000001.sdmp	JoeSecurity_RMSRemote Admin	Yara detected RMS RemoteAdmin tool	Joe Security	
0000000B.00000003.319348250.000000007E8F 0000.00000004.00000001.sdmp	JoeSecurity_RMSRemote Admin	Yara detected RMS RemoteAdmin tool	Joe Security	
0000000B.00000000.293269223.000000000120 8000.00000002.00020000.sdmp	JoeSecurity_RMSRemote Admin	Yara detected RMS RemoteAdmin tool	Joe Security	
Click to see the 10 entries				

Sigma Overview

System Summary:

- Sigma detected: Execution from Suspicious Folder
- Sigma detected: Microsoft Office Product Spawning Windows Shell
- Sigma detected: Suspicious WMI Execution
- Sigma detected: Net.exe Execution

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

- Document exploit detected (drops PE files)
- Document exploit detected (UrlDownloadToFile)
- Document exploit detected (process start blacklist hit)

System Summary:

- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Contains functionality to create processes via WMI
- Found abnormal large hidden Excel 4.0 Macro sheet
- Office process drops PE file

Persistence and Installation Behavior:

- Creates processes via WMI

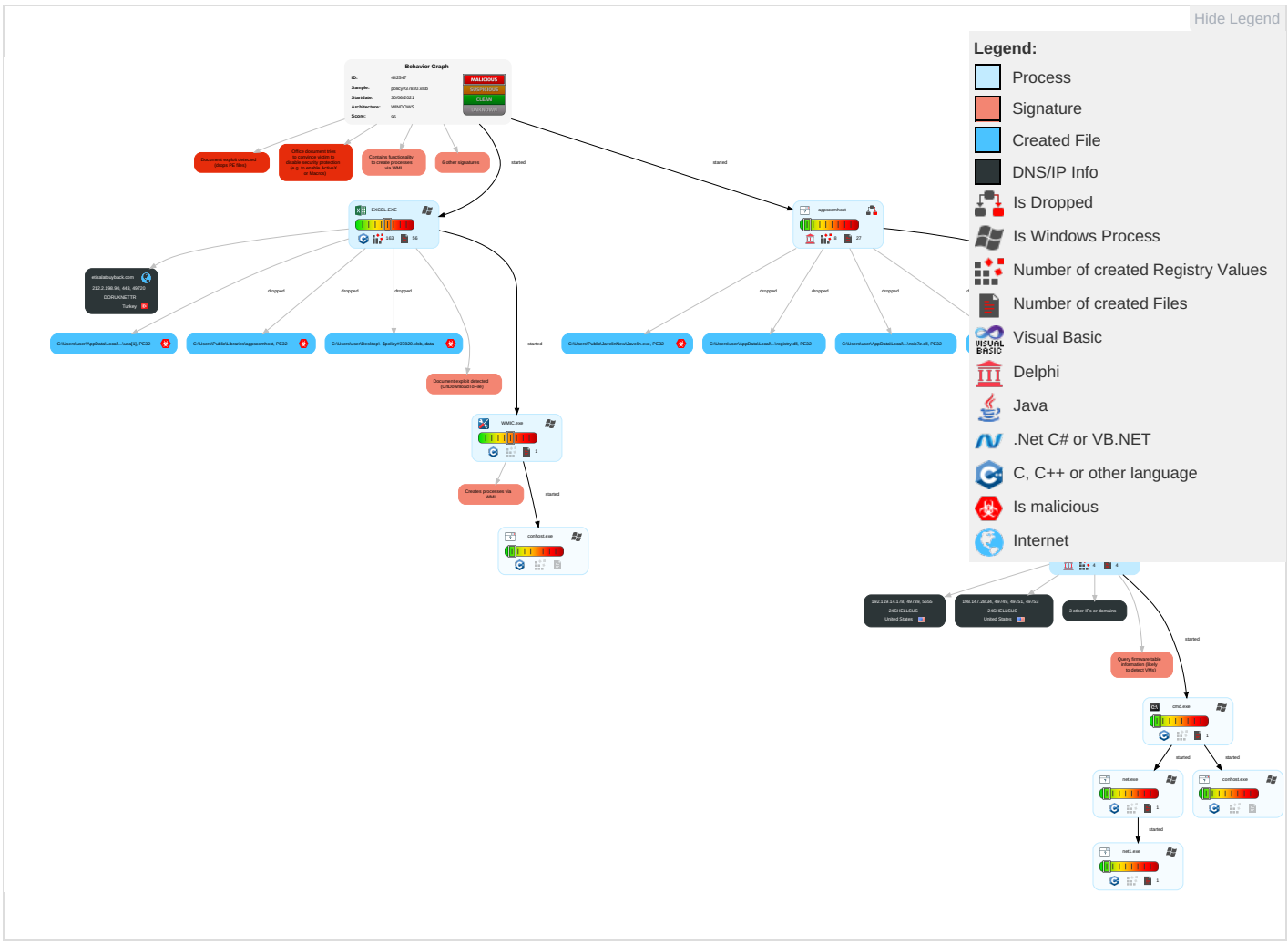
Malware Analysis System Evasion:

- Query firmware table information (likely to detect VMs)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Scripting 1	LSASS Memory	System Information Discovery 3 7	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Access Token Manipulation 1	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applic Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 1	DLL Side-Loading 1	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applic Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comn
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comn Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 1 1	/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)	Access Token Manipulation 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

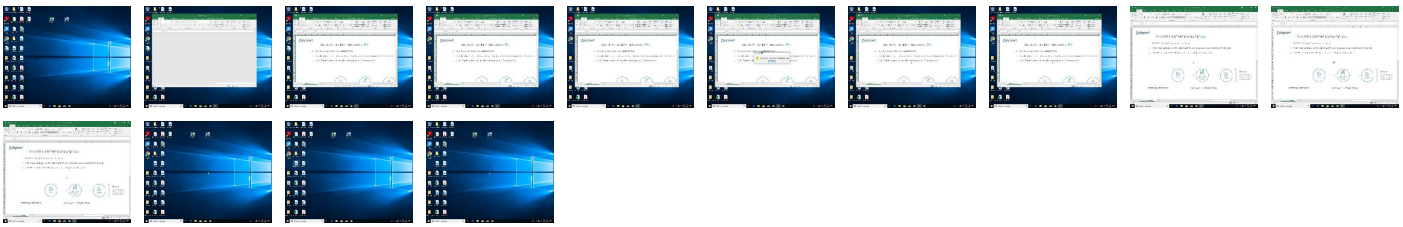
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\JavelinNew\libeay32.dll	3%	Metadefender		Browse
C:\Users\Public\JavelinNew\libeay32.dll	3%	ReversingLabs		
C:\Users\Public\JavelinNew\ssleay32.dll	0%	Metadefender		Browse
C:\Users\Public\JavelinNew\ssleay32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso349F.tmp\NSISList.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso349F.tmp\NSISList.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso349F.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso349F.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso349F.tmp\nsis7z.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nso349F.tmp\registry.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso349F.tmp\registry.dll	2%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.1.appscomhost.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
etisalatbuyback.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://update.remoteutilities.net/upgrade_beta.ini	0%	Virustotal		Browse
http://update.remoteutilities.net/upgrade_beta.ini	0%	Avira URL Cloud	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://www.indyproject.org/	0%	URL Reputation	safe	
http://madExcept.comU	0%	Avira URL Cloud	safe	
http://update.remoteutilities.net/upgrade.ini	0%	Virustotal		Browse
http://update.remoteutilities.net/upgrade.ini	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
etisalatbuyback.com	212.2.198.90	true	false	• 0%, Virustotal, Browse	unknown
id70.remoteutilities.com	209.205.218.178	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.119.14.178	unknown	United States		55081	24SHELLSUS	false
198.147.28.34	unknown	United States		55081	24SHELLSUS	false
209.205.218.178	id70.remoteutilities.com	United States		55081	24SHELLSUS	false
212.2.198.90	etisalatbuyback.com	Turkey		8685	DORUKNETTR	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	442547
Start date:	30.06.2021
Start time:	20:05:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	policy#37820.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	29
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:	mal96.expl.evad.winXLSB@15/18@4/6
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 66.4% (good quality ratio 65.2%) • Quality average: 88% • Quality standard deviation: 19.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • 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
20:06:11	API Interceptor	1x Sleep call for process: WMIC.exe modified
20:06:23	API Interceptor	17x Sleep call for process: Javelin.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.119.14.178	Webinar.exe	Get hash	malicious	Browse	
	QBikGim.exe	Get hash	malicious	Browse	
	FG1eBAAwpR.exe	Get hash	malicious	Browse	
	04_12_21.exe	Get hash	malicious	Browse	
209.205.218.178	etcglobal.odt.exe	Get hash	malicious	Browse	
	Desktop.exe	Get hash	malicious	Browse	
	04.12.21.exe	Get hash	malicious	Browse	
	Webinar.exe	Get hash	malicious	Browse	
	QC-Telecom.exe	Get hash	malicious	Browse	
	4CyHW6t6Yr.exe	Get hash	malicious	Browse	
	QBikGim.exe	Get hash	malicious	Browse	
	FG1eBAAwpR.exe	Get hash	malicious	Browse	
	04_12_21.exe	Get hash	malicious	Browse	
	8XioA9UTsz.exe	Get hash	malicious	Browse	
	8XioA9UTsz.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
id70.remoteutilities.com	etcglobal.odt.exe	Get hash	malicious	Browse	• 209.205.218.178

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
24SHELLSUS	etcglobal.odt.exe	Get hash	malicious	Browse	• 209.205.218.178
	HuPjcvVze1.exe	Get hash	malicious	Browse	• 67.220.184.242
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 67.220.184.98
	PO108021.exe	Get hash	malicious	Browse	• 108.175.160.242
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 67.220.184.98
	New Order202105.exe	Get hash	malicious	Browse	• 67.220.184.98
	IQ4lblwCjQ.exe	Get hash	malicious	Browse	• 67.220.184.98
	sample products 1,2,&,4.exe	Get hash	malicious	Browse	• 209.205.207.130
	PO QT-028564.xlsx	Get hash	malicious	Browse	• 67.220.184.98
	IMG_20210526_SWIFTOREPORT_JPG.exe	Get hash	malicious	Browse	• 67.220.184.98
	TNT ADVICE.docx	Get hash	malicious	Browse	• 67.220.184.98
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 67.220.184.146
	Shipping Details.exe	Get hash	malicious	Browse	• 67.220.184.98
	TNT BILL OF LADING DOCUMENTS.exe	Get hash	malicious	Browse	• 67.220.184.98
	Invoice#0593.exe	Get hash	malicious	Browse	• 67.220.184.98
	Invoices.exe	Get hash	malicious	Browse	• 67.220.184.98
	INV_6682738993_IMG.exe	Get hash	malicious	Browse	• 67.220.184.98
	VWR CI 220221.xlsx.exe	Get hash	malicious	Browse	• 67.220.184.98
	file.exe	Get hash	malicious	Browse	• 67.220.184.98
	Shipping DetailsPDF.exe	Get hash	malicious	Browse	• 67.220.184.98
24SHELLSUS	etcglobal.odt.exe	Get hash	malicious	Browse	• 209.205.218.178
	HuPjcvVze1.exe	Get hash	malicious	Browse	• 67.220.184.242
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 67.220.184.98
	PO108021.exe	Get hash	malicious	Browse	• 108.175.160.242
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 67.220.184.98
	New Order202105.exe	Get hash	malicious	Browse	• 67.220.184.98
	IQ4lblwCjQ.exe	Get hash	malicious	Browse	• 67.220.184.98
	sample products 1,2,&,4.exe	Get hash	malicious	Browse	• 209.205.207.130
	PO QT-028564.xlsx	Get hash	malicious	Browse	• 67.220.184.98
	IMG_20210526_SWIFTOREPORT_JPG.exe	Get hash	malicious	Browse	• 67.220.184.98
	TNT ADVICE.docx	Get hash	malicious	Browse	• 67.220.184.98
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 67.220.184.146
	Shipping Details.exe	Get hash	malicious	Browse	• 67.220.184.98
	TNT BILL OF LADING DOCUMENTS.exe	Get hash	malicious	Browse	• 67.220.184.98
	Invoice#0593.exe	Get hash	malicious	Browse	• 67.220.184.98
	Invoices.exe	Get hash	malicious	Browse	• 67.220.184.98
	INV_6682738993_IMG.exe	Get hash	malicious	Browse	• 67.220.184.98
	VWR CI 220221.xlsx.exe	Get hash	malicious	Browse	• 67.220.184.98
	file.exe	Get hash	malicious	Browse	• 67.220.184.98
	Shipping DetailsPDF.exe	Get hash	malicious	Browse	• 67.220.184.98

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Q8RJQ90EC6.exe	Get hash	malicious	Browse	• 212.2.198.90
	H03PtcViQG.exe	Get hash	malicious	Browse	• 212.2.198.90
	banka bildirimi SWIFT PDF.exe	Get hash	malicious	Browse	• 212.2.198.90
	yKz3gtwWvN.exe	Get hash	malicious	Browse	• 212.2.198.90
	Mz89FW9zvK.exe	Get hash	malicious	Browse	• 212.2.198.90
	data.doc_Client.exe	Get hash	malicious	Browse	• 212.2.198.90
	obfuscated-html.html	Get hash	malicious	Browse	• 212.2.198.90
	MV YU FENG4 TRADER_ISO8217.docx	Get hash	malicious	Browse	• 212.2.198.90
	plan-870783614.xlsb	Get hash	malicious	Browse	• 212.2.198.90
	newbad.rtf_Client.vbs	Get hash	malicious	Browse	• 212.2.198.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	spot.dll	Get hash	malicious	Browse	• 212.2.198.90
	spot.dll	Get hash	malicious	Browse	• 212.2.198.90
	3.dll	Get hash	malicious	Browse	• 212.2.198.90
	3.dll	Get hash	malicious	Browse	• 212.2.198.90
	StsDQGUVmT.exe	Get hash	malicious	Browse	• 212.2.198.90
	L0DdbYIYEx.exe	Get hash	malicious	Browse	• 212.2.198.90
	GamDzCDMI0.exe	Get hash	malicious	Browse	• 212.2.198.90
	O8O8CUUvAF.exe	Get hash	malicious	Browse	• 212.2.198.90
	1.htm	Get hash	malicious	Browse	• 212.2.198.90
	plan-515372324.xlsb	Get hash	malicious	Browse	• 212.2.198.90

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\JavelinNew\libeay32.dll	etcglobal.odt.exe	Get hash	malicious	Browse	
	english.exe	Get hash	malicious	Browse	
C:\Users\Public\JavelinNew\ssleay32.dll	etcglobal.odt.exe	Get hash	malicious	Browse	
	english.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\JavelinNew\Javelin.exe	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16615672
Entropy (8bit):	6.76564442538193
Encrypted:	false
SSDEEP:	196608:HNjzJSeEtAVBt4/BixizJcPM5OzQ6UM6pZpKerXvob24wwMIbQEWn:HNjzJSeE0D4KiZ5OyM6pXTrXvVw/bQEe
MD5:	AF5879D56594F01794A2C028BC75EC27
SHA1:	27AB93CA87C9F13EC6425916C3F15AD96AF92A8D
SHA-256:	41108849FEA92A7E8085BF312EE721145A50C105F8B7B41BBB743C4B6B643927
SHA-512:	F6C60BA983777B683D2DB4E1C0DBD2B9CDA3ED83D96997947798AC4ACE9E52DB71F144565C85225E01BBD79FF13BADFF392D2A656F83C026DF92575CEA7D6AEF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Users\Public\JavelinNew\Javelin.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\Public\JavelinNew\Javelin.exe, Author: Joe Security
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....;`.....R....,.....e.....p....@.....\_w.....@.....`.....\...`...k.....d.....T..... .....}.....text..... ..`.itext...u.....v..... ..`.data.....p.....V.....@....bss....T.....idata...\.....^...Z.....@....didata..}..... .~.....@....edata.....`.....6.....@..@.tls....h....p.....rdata..].....8.....@..@.reloc..T.....:.....@..B.rsrc....k...`...l.....@..@..... .....@..@.....

C:\Users\Public\JavelinNew\inst801.7z	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	644
Entropy (8bit):	7.52900611913228
Encrypted:	false
SSDEEP:	12:g85ORiuXW33K331d5zMd97plmRe7HDjq8hLTY661ROMcSna4FLIPwgy:h5OoY8mgFp0Qvq8KBrdYwgy
MD5:	9E9AAAC7CA998A5C55B9578FA4241C0A
SHA1:	31CE8220671FB47D91A6A391AB80E49C962A881F
SHA-256:	A5A4F0E2DA4C479B4D056985B5E71EF7F69D4BDD6AD04255794ACA9A7AA648D1
SHA-512:	6333BBFB126680C39B0DE260F6BB61303D2F953D4EC4FD74C43162B4E1B7BB77BFEB9671623E40B4E5B2628232325198FF46C65E57A2DA10A0BE04104E368FEE
Malicious:	false
Preview:	7z..'.....A.....#.....a.h.*..$.fw.....\..8...}..m...?...;O.P/..2.V....~/E.VsmfD>c.....T..>.s.C.,.....;J.....0.I%.I..JN65.h .&.. .,.....O.U084>.....!{?..[..@`..p.7\..L..nI..)....A....Y5 .F...3..._.{G..%..e|..9...W...}_G. .V.g:GX_rt1.....".u:.....3.Ra..\|vrR....!.6....j:.'...M..vrY.v.S....Z.y.a.Pt..bD.sm....n.....,.....e.j.fz...{..}U..9.GC....$_+Yu2j).P.R..Q...n[..._.W.D.n Rx.X.....I.G.GL.....3...o.>I.b:...CLW...%.8~.r..g..\...-.p..,..dQ....X.>.J...L..n.c.G...sB%....X.....:.....&T.).0..)..%=.S.I..JC...x....j..d.[.5.xs...f.[\!.~..D.6Z.nX .7..T;o.`.^U....n}{..p... .....#....]......J...c}...

C:\Users\Public\JavelinNew\instzip594.7z	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	5154900
Entropy (8bit):	**7.99995626098956**
Encrypted:	**true**
SSDEEP:	98304:GDNvXLvCK5oW+DiqwEZzwoVTU38+hAByZApTjxEtSJ94+PrJhWX7a8ap0GAJ6:mLvCK6i+3UdQdPx2A9p8g07o
MD5:	49A827B49E2E110EEC4E4522D301B69B
SHA1:	474EC31448E05CEA5F285C933504E05435790056
SHA-256:	FADBD996888FC88D709DCEB923D9DDFDAF82A09D2FC514B39974E6740AED8AA1
SHA-512:	5E95937F2F1AFEFE324CB954632B4449DD304AD5779B7D07B00172244E431CE4B0CC055AE319801720C1E9B582F5744850F7E410A7ED0D0EEA5DC1262C84AB9
Malicious:	false
Preview:	7z..'...%..v..N.....%.....&.....k.u....{.:....Rd...<-WG.-.....o%..P..[.R..|=LuM...s....q/p_.%o.....j....*#..oB.+E...HM..w..d?Wg`X.....gB."2.A;.K...\...I...X.J.....!...,...#...^..0/...0=r ..]\.|.....A..Q~l... 3..!..?]..#z..[1.....K.s0..Rd....0^.&+.8.+..[.c.kn.....E$.[.\.d.....u.P..~S..\|".....pS....S_.....Up..^$.....fSUGe.....N.Alg.A..o/T..*.R.7..Pn.y@.iWx[.I..W....FX..3.T U_....".n1.wLb.L.'.?A.....c.Z..0..5.}..d.l7n.....$!...F.Q.~.n..>1.!.^n.....:....\|..zF.a.v.$..a....J .6.`..7...a.O,<r..7....$.34.....l'...2.9..URG.z....?v..t].u1.5o...lx.....f.N9.....P.:b..7.$.... ....]]..... .....:...(.1.dY.-&.[.,... .t.....6.<..(F.C...k."....:Q..N..*d.C.*]J...y..XPl.t...HF ....}..PO5....YC.b....{...x...o[..... ...p.C.;..Z..._..(4._...7.?.T.s.@.N.R.z....A,.....U....f.~...h.r..6. !..DeL..C.R...}....m..Vt.-3..%~...FP..E.pU...i.8..h..I...hk.....0.....}bb.~.$U..e.4c.,...'rAj..A]a...+..+?..c.Yj.$..7d...J.R.ew.*...~....r[.~e.P..8P..Fb..[,...i..z.@x}..

C:\Users\Public\JavelinNew\libeay32.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1377016
Entropy (8bit):	6.8566450434786255
Encrypted:	false
SSDEEP:	24576:nD8B+KpPexB6mqwktXUcAVEaFQXhL0porIqo+FrzbN:EKkmlktXUcAVEDhQporIqo+FrzbN
MD5:	0D51927274281007657C7F3E0DF7BECB
SHA1:	6DE3746D9D0980F5715CEC6C676A8EB53B5EFC49
SHA-256:	DFC847405BE60C29E86E3E3222E7F63C1FF584727D87D3C35C25C4893E19FDA0
SHA-512:	EEF74088A94635184192D82BB6DCC0758749CB290C8DEEFF211881E8A280AEC73A53334EFF8846DF618204B0F318E757EAB23E76951A472BA6E086905000D9A5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 3%
Joe Sandbox View:	• Filename: etcglobal.odt.exe, Detection: malicious, Browse • Filename: english.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b7.j&V.9&V.9&V.9/..9.V.9/..9=V.9&V.9.V.9...9-V.9&V.93V.9/..9.T .9/..9'V.9/..9'V.9/..9'V.9Rich&V.9.....PE..L.....Y.....!.....\.....p.....P.....[.....r.....x.....0.....P...pr..... .....p...@.....p..(.....text....[.....\..... ..`.rdata...X...p...Z..`.....@..@.data.....t.....@....rsrc...0.....@..@.reloc..... .....4.....@..B..... .....

C:\Users\Public\JavelinNew\ssleay32.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	345336
Entropy (8bit):	6.557003324106128
Encrypted:	false
SSDEEP:	6144:IEXfWSXFKIsrpivdM+kPsmWak8dfthPDP0wrE90k7DUT/NaDB7JlwScihgbX5/Gd:IEXfWSVKIsrpivdM+msmWak8dfnPDPPG
MD5:	197DA919E4C91125656BF905877C9B5A
SHA1:	9574EC3E87BB0F7ACCE72D4D59D176296741AA83
SHA-256:	303C78ABA3B776472C245F17020F9AA5A53F09A6F6C1E4F34B8E18E33906B5EE
SHA-512:	33C1B853181F83CAB2F57F47FB7E093BADF83963613E7328EBD23F0D62F59416D7A93063C6237435FBB6833A69BC44EBBC13AA585DA010F491C680B2EA335C47
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: etcglobal.odt.exe, Detection: malicious, Browse • Filename: english.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...r...r.....r.....r.....r.....r...s.6.r....\.r.....r.....r.....r.Rich..r.. .....PE..L.....Y.....!.....l.....Y3.....S.....0....).....<....0..0.....&.....@....,..0.....0...@..... .....text...Z..... ..`.rdata.....@..@.data....[.....@.....@....rsrc...0....0.....@..@.reloc...3...@...4.....@..B..... ....

C:\Users\Public\Libraries\appscomhost	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\Public\Libraries\appscomhost	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	5437775
Entropy (8bit):	**7.998224982007381**
Encrypted:	**true**
SSDEEP:	98304:oY+ZDNvXLvCK5oW+DiqwEZzwoVTU38+hAByZApTjxEtSJ94+PrJhWX7a8ap0GAJa:oNLvCK6i+3UdQdPx2A9p8g07Rq
MD5:	8DF649FAB065908962626C67F247618C
SHA1:	19EBC4AA4CC9823788746394EC8419047B43EAE9
SHA-256:	FD4514FF3A7DC34574A19042EC70947136137B853C3EC4D7155123562627F450
SHA-512:	7346E89005AA5279FE05372C9A18B749173313639994B2C45EC4240864B3D70F8B183757B9714F43559F9B3B2799ABC4E315994BB80D88F09EC74C434EC7D094
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.$_.....h...:...@...4.....@.....0 .....@.....0f..... .....text....g.....h..... ..`.rdata.....l.....@..@.data.....@....ndata.....rsrc...0f.....h.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\662FAE06-B8BB-4FD3-9343-79CB8671E669	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135209
Entropy (8bit):	5.363061097155553
Encrypted:	false
SSDEEP:	1536:VcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:hEQ9DQW+zwXO1
MD5:	05894699F3058B23A6AD101179A32F6E
SHA1:	7BAD5520501DF94673D112DBFEE2BB0F52ADFF42
SHA-256:	75CE9E41FAF69192D34DE599A31D53B4ABC52C57483A77490BC8766DE400EC64
SHA-512:	126D91DC63E60E002F2EC765131E13BD664D3FD48524FB8F6B2945D16AABFD32DDDE463E8F522EE8395C76CB103B15255F4B9D3F0F5FBD2A20B72300727A8FE D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-30T18:06:00">.. Build: 16.0.14228.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\85BBDE0D.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 2260 x 952, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	81517
Entropy (8bit):	7.942268293903438
Encrypted:	false
SSDEEP:	1536:PnIciz38MXwe/g/aGLb6QT/Y+mhu9JOERaXwfSLfGrBvMNK/rEE5ZYU8lMz4rNV/:PnIcA38Y/UzzFmMeyagf8unr5h8Y4rNN
MD5:	9DB42D5B391AE2498C4C6E77B7A06F19
SHA1:	7E93865DA631CE7342EEC7E90D2FEF83485F78F0
SHA-256:	60F4BFE9CB33E34C4D50943E3A0DFC1AE7EDA2A97A6192AC3CC4BD34ABEF76EA
SHA-512:	D8D96C4005B2B4C35A7D3F87B48FDBD0B72059E664234DD76A7CF5DEE6F2FEFBC5D6E75A8892B3251DC7021125BEA89CC71F012B3C54915B42C83CD2389D4 C
Malicious:	false
Preview:	.PNG.....IHDR.....'.....gAMA.....a.....sRGB.....pHYs...t...t..f.x...rPLTE.....wxy.....KJJ888.....ZZZ.....%%%jjj.q.....-..J..3a....g.....i.....8..z.m. G....=.IDATx....H.....^J.).bV.....R'@..vLx....X.Z".....4.....OO..^.....U3.sh.....j.../.g...e .#.....y..).....6..M|=._'...3..12.....$....:_.4.{.dM].....1..L#..s.f.>%v.i_.....{NE$..r.....2.Y...T.....1.....k'...5.<.jt...u(.j.....jb(.....|qKw~.....&.....Z._..-~....V..+P.k."6'...^#.K)9.|.... [...Z%./.....5y...4.5).....E.4..P."...@c~BO.>ac..n*.Vo..^.X...N...'.q.....2.Ta...v.T..$.!....'..Luo.....^...].Q.q]?.7.O6.....La.....A".J.Z....E]..}..#..L."V.>./m{...j..x9!.....0N.c5.c.DU..E O.b.j..v:.o..R...t..v.?.=...^-..LDly8\.....B....$...hY.Jxl...h.\s.{gT.S..H.T.....)}.5..7.....HC.Q.[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B065FF3C.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1108
Entropy (8bit):	2.025265777483207
Encrypted:	false
SSDEEP:	12:Y8uOvplqCHJ/duThp0p1hpk1Z/ux0tL9IgkXfRkMXI3ioyaf:YXeOCp/dI0p/pYux8LVkWty6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B065FF3C.emf	
MD5:	C5333859687EFA952470EAA98027A042
SHA1:	4FF7D216CA84BEF4E4C5448B879EF8F6F5C5A476
SHA-256:	1D4B6D5B8718DD67596BF8414C6F47D8FAAC6C90FC05622D0634170AB4D4A429
SHA-512:	A17327739A17FBDCCF455AEF0F80B6099AFC54088BE447A15A25C4B8816087F46E4E3FCFB516527893DF9A2002B7878E02A3F4DC01007BFC26AC380E7E874338
Malicious:	false
Preview:	....l.....2... EMF....T.....8...X.....?.....F.....GDIC.....?B".....d.....ddd.....-.....!..... ..!.....!.....!.....-.....!.....'.....ddd....%.....L...d..... ....!.....?.....?.....L...d.....!.....?.....?.....L...d.....!.....?.....?..... ....L...d.....!.....?.....?.....'.....%.....L...d.....!.....?.....?.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\usa[1]	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	5437775
Entropy (8bit):	**7.998224982007381**
Encrypted:	**true**
SSDEEP:	98304:oY+ZDNvXLvCK5oW+DiqwEZzwoVTU38+hAByZApTjxEtSJ94+PrJhWX7a8ap0GAJa:oNLvCK6i+3UdQdPx2A9p8g07Rq
MD5:	8DF649FAB065908962626C67F247618C
SHA1:	19EBC4AA4CC9823788746394EC8419047B43EAE9
SHA-256:	FD4514FF3A7DC34574A19042EC70947136137B853C3EC4D7155123562627F450
SHA-512:	7346E89005AA5279FE05372C9A18B749173313639994B2C45EC4240864B3D70F8B183757B9714F43559F9B3B2799ABC4E315994BB80D88F09EC74C434EC7D094
Malicious:	**true**
IE Cache URL:	http://https://etisalatbuyback.com/static/docs/usa
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.$_.....h...:..@...4.....@.....0 .....@.....0f..... .....text....g.....h..... ..`.rdata.....l.....@..@.data.....@....ndata.....rsrc...0f.....h.....@..@..... ....

C:\Users\user\AppData\Local\Temp\53B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	683257
Entropy (8bit):	7.744604873577989
Encrypted:	false
SSDEEP:	6144:1cvH5bJDPDYdx4wK8IOhQpHKecN/UzzGyXjnr5YrNVo9Y/GbH:18bA08IOhOHuNUnGyznrGrNVE+GbH
MD5:	733B6623ABD138741A1483FDDC1C2C2F
SHA1:	D7A885906FB7A565B3A352DEA8DAE7C20E1297E1
SHA-256:	DD4088AB798B2D00AA210E2710B946C768262140CD59656599F8EB2B5126F284
SHA-512:	FD3C5ADBD82F53B7368DEF4CFBF16BDEE65783B778EBDAFECC3BC4C31FBEA3CBECF45F991A3CC3D0D046AA85AAFE819877DBC8AA56CCD09AE5B3BB2778D41F6B
Malicious:	false
Preview:	.UIo.0..#..''_Q.)...dz....(.W..2..lw...<;i..I.M/.oy.....BT.6.H.V8..!?...I....kg.!G..z.....!V...!]J..cQt`x.....\.....&..N..I.7.....?.N....._.j..^+...e.+...k[%.r...~.6.....2.I.>...N".:.Lc..`...cF("KP.S>...P.+.3r.w...L.06dU:.`.H..7.?bCdc.W..P..r..a.f.....n...4v.....|..k.}J..RAFVnWgH...}.....4GR..|...e.>.....F.fY.K.....+'w]R.x..=.l.W7.'...9t}d...y...t.q...9....9...w...c8....inet..BR.<...."...;..!!ANh.r(m~.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	248808
Entropy (8bit):	4.293878216916494
Encrypted:	false
SSDEEP:	1536:X8pwK20L0SlWWZFVKKHaRRDqBcAQHdHTuETaK/E5A0j3kTkJlsDWpksZk/6tf2Dy:XC38WZFVKKHSRDqBcA+FLM0Ar6t3s6bh
MD5:	69139435A54B77B8C578A3ABED32BEC4
SHA1:	EB55DC8452DEA5AE616289BD790E99D8DB5994BF
SHA-256:	73A5512B7BD0DCACC02E5AEFB4C248C86B284C719B5A4A19E85B68F739B3DCE0
SHA-512:	0E7B5FA53EDCFBE757F0FF12990388D73C6D662243AA796072BC42B3F93C7575639561266E423B1FEAB9A16B3EB262EA9A6CD9CC7BE27B36A3D318D61C68193
Malicious:	false

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Preview:	MSFT.....Q.....%.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"...".(#...#...#..T$...$...%...% ...%..H&...&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9.. 4:...:...:..`:...;..(<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....l...B.....H...4..... .....x..lL.....T..... ....P..... .....

C:\Users\user\AppData\Local\Temp\nso349F.tmp\NSISList.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107520
Entropy (8bit):	6.399584175418038
Encrypted:	false
SSDEEP:	3072:YJSzh02DsLMtTmDW2qTKh1kOLoLYidGlSf9:wSS2DkYQqTHTdGl
MD5:	49BB98396DC0187146319F8C130C363C
SHA1:	548F11A0BA951291656DA67BA5A49C439A87130B
SHA-256:	517A328BFED8935773D94A40812763CCDF08881AD5D71A83A629EAFA62B41CF2
SHA-512:	290D87D644707A7096613CBA4EB84F7E23F426BF98D8540DEF6A76AC748E4EEB34C7E2FAABB39B602B2DEF604535CD574CE35ED15E346CF43B544FDBBAEA94 58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 4%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....X...H.....r.....@.....0.....J..... .....text...R.....T..... ..`.itext.....p.....X..... ..`.data.....\.....@....bss.....3.....j.....idata..J.....j.....@....edata..... .....v.....@..@.reloc.....x.....@..B.rsrc.....@..@.....0.....@..@..... .....

C:\Users\user\AppData\Local\Temp\nso349F.tmp\System.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.737504888129487
Encrypted:	false
SSDEEP:	192:BenY0qWTlt70IAj/lQ0sEWc/wtYbBH2aDybC7y+XB9IwL:B8+Qlt70Fj/lQRY/9VjjlL
MD5:	8CF2AC271D7679B1D68EEFC1AE0C5618
SHA1:	7CC1CAAA747EE16DC894A600A4256F64FA65A9B8
SHA-256:	6950991102462D84FDC0E3B0AE30C95AF8C192F77CE3D78E8D54E6B22F7C09BA
SHA-512:	CE828FB9ECD7655CC4C974F78F209D3326BA71CED60171A45A437FC3FFF3BD0D69A0997ADACA29265C7B5419BDEA2B17F8CC8CEAE1B8CE6B22B7ED9120BB AD3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....]..... ....)..... .....@.....p.....@.....B.....@..P.....`.....@..X. .....text...O ..... ..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nso349F.tmp\nsis7z.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	179496
Entropy (8bit):	6.484752992108191
Encrypted:	false
SSDEEP:	3072:Z76+sYX+bTOybVJJhk6BoUDReZgbUP3A4zeGh62RZ56GMX:Zvs8+WeVJQ6CUDRe+UPAYefimRX
MD5:	7CD97D946E10E902ED2822508E2A11C4
SHA1:	FC64D292D1C239ABC82BB49A063A58FF8D0609FB
SHA-256:	F2FC2A430833ED9FEF374EC73CB3302D66471AAADDB2F63D3E6E4139B212B78B
SHA-512:	52513E03FDB79EAEB3D43D28F6862515C13AD65483A2786CA4AA4E5B1EAA5E34AD3C627B9B1BFB5F89B192CDC1C6B6073F3B34BCE36FD2FABF6D286E139876 21
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nso349F.tmp\nsis7z.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r.S.6.=S6.=S6.=S(..S..=S(..S!.=S(..SB.=S.<PS7.=S.<FS?.=S6.<S..=S?..S7.=S(..SX.=S(..S7.=S(..S7.=S(..S7.=SRich6.=S.....PE..L...C..M.....!.....u.....V.....m.....c..P.....(.....h.....0:..@.....text..... ..`.rdata...^.....^.....@..@.data....^...p.....Z.....@....rsrc.....r.....@..@.reloc...-.....|.....@..B.....

C:\Users\user\AppData\Local\Temp\nso349F.tmp\registry.dll	
Process:	C:\Users\Public\Libraries\appscomhost
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	6.16866702253594
Encrypted:	false
SSDEEP:	384:W2mvyNjH3rPnAZ4wu2QbnC7qB7PnrvScaeYA4CIDEge/QqL2AQ:/75w/OfrzB4CUxuQfA
MD5:	2B7007ED0262CA02EF69D8990815CBEB
SHA1:	2EABE4F755213666DBBBDE024A5235DDDE02B47F
SHA-256:	0B25B20F26DE5D5BD795F934C70447112B4981343FCB2DFAB3374A4018D28C2D
SHA-512:	AA75EE59CA0B8530EB7298B74E5F334AE9D14129F603B285A3170B82103CFDCC175AF8185317E6207142517769E69A24B34FCDF0F58ED50A4960CBE8C22A0AC/
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..]...]..]..|R..]...]...]...Q..]...Q..]...Q..]..Rich.]..... .....PE..L...PxEN.....!.....H... .....#.....`.....i.....f..P.....<.....`.....text....G.....H..... ..`.rdata.....`.....L.....@..@.data.....p.....X.....@....reloc.....Z.....@..B.....

C:\Users\user\Desktop\~$policy#37820.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1Mgkd3vs36JQAiveyn:Yw7gJGWMXJXKSOdYiygKkXe/egkZ0qeF
MD5:	7A172F8E10BA6DDE2024BC3F01C484A9
SHA1:	CD9718A5A66042CE7D0124293E48793BFFA78A6B
SHA-256:	DE0F24AC9C3F7519230115A6EFC2AC06C5B87746E3CD543C9DEC05511E1BC56D
SHA-512:	1B05B19B38331D14CFEE92B9E7AF0C95018E9306859646633F2CB942023A34ECEDE7AB4EBE80576A34D57772FF7C49F49F1292263A1C7FFE1386787A3303F473
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6596;...ReturnValue = 0;..};....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.909878787236229
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.73% • Excel Microsoft Office Open XML Format document (40004/1) 41.88% • ZIP compressed archive (8000/1) 8.38% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	policy#37820.xlsb
File size:	123671
MD5:	f60146ee4fab89ecde8bb1bdb23287b6
SHA1:	82bb4929a849deb1860e4c902745a0673c5911c8
SHA256:	6ab90a34f6fdfaf1486009f70318816cc61201248c0a5231030b9b3d3e010fe9
SHA512:	d88c89b05aac6cde9feb51fc3e43d193747befbabc411001565bff1ab8c2ee03767d9451ed357d47cb6394930cda34a0714e1eebfbef024430ff5dc67c847063
SSDEEP:	3072:iu+RyXneul60EHA/djFCmQQ26ysWD5mcJU0vBA7eyX0fp0KpqY8C:iuJeutEqrv9K
File Content Preview:	PK.....}..R.....docProps/PK.....R.....docProps/app.xml.SAn.0.....hB@N1.....fP..rh..v.3K.,"4)p7..G..}Y).....F....hvD....."..'|..9.oBa.j.....8C....x..- .Q.?.Y.5D...,lx.....~.}B....R.W"..50..e...U._..... ._.....h.L...

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "policy#37820.xlsb"

Indicators

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

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2021 20:06:07.509063959 CEST	192.168.2.3	8.8.8.8	0x6247	Standard query (0)	etisalatbuyback.com	A (IP address)	IN (0x0001)
Jun 30, 2021 20:06:49.682568073 CEST	192.168.2.3	8.8.8.8	0x61ee	Standard query (0)	id70.remoteutilities.com	A (IP address)	IN (0x0001)
Jun 30, 2021 20:06:55.366902113 CEST	192.168.2.3	8.8.8.8	0x9afd	Standard query (0)	id70.remoteutilities.com	A (IP address)	IN (0x0001)
Jun 30, 2021 20:07:40.818829060 CEST	192.168.2.3	8.8.8.8	0xd78a	Standard query (0)	id70.remoteutilities.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2021 20:06:07.603307962 CEST	8.8.8.8	192.168.2.3	0x6247	No error (0)	etisalatbuyback.com		212.2.198.90	A (IP address)	IN (0x0001)
Jun 30, 2021 20:06:49.742058039 CEST	8.8.8.8	192.168.2.3	0x61ee	No error (0)	id70.remoteutilities.com		209.205.218.178	A (IP address)	IN (0x0001)
Jun 30, 2021 20:06:55.414963007 CEST	8.8.8.8	192.168.2.3	0x9afd	No error (0)	id70.remoteutilities.com		209.205.218.178	A (IP address)	IN (0x0001)
Jun 30, 2021 20:07:40.867377043 CEST	8.8.8.8	192.168.2.3	0xd78a	No error (0)	id70.remoteutilities.com		209.205.218.178	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 30, 2021 20:06:07.826231956 CEST	212.2.198.90	443	192.168.2.3	49720	CN=etisalatbuyback.com, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jul 16 13:21:56 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:39:16 CEST 2004	Wed Aug 25 11:11:38 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jun 29 19:39:16 CEST 2004	Thu Jun 29 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5412 Parent PID: 792

General

Start time:	20:05:57
Start date:	30/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xa50000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 6388 Parent PID: 5412

General

Start time:	20:06:10
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create 'C:\Users\Public\Libraries/appscomhost'
Imagebase:	0xdf0000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 6448 Parent PID: 6388

General

Start time:	20:06:10
Start date:	30/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: appscomhost PID: 6596 Parent PID: 4940

General

Start time:	20:06:12
Start date:	30/06/2021
Path:	C:\Users\Public\Libraries\appscomhost
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Libraries/appscomhost
Imagebase:	0x400000
File size:	5437775 bytes
MD5 hash:	8DF649FAB065908962626C67F247618C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: Javelin.exe PID: 6832 Parent PID: 6596

General

Start time:	20:06:18
Start date:	30/06/2021
Path:	C:\Users\Public\JavelinNew\Javelin.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\JavelinNew\Javelin.exe'
Imagebase:	0x400000
File size:	16615672 bytes
MD5 hash:	AF5879D56594F01794A2C028BC75EC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000008.00000002.300472994.0000000001208000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000008.00000000.273261388.0000000001208000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000008.00000002.294909755.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000008.00000000.268064699.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\Users\Public\JavelinNew\Javelin.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\Public\JavelinNew\Javelin.exe, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Javelin.exe PID: 7128 Parent PID: 6832

General

Start time:	20:06:28
Start date:	30/06/2021
Path:	C:\Users\Public\JavelinNew\Javelin.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\JavelinNew\Javelin.exe -run_agent -second
Imagebase:	0x400000
File size:	16615672 bytes
MD5 hash:	AF5879D56594F01794A2C028BC75EC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 0000000B.00000003.311749860.000000007D910000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 0000000B.00000003.319348250.000000007E8F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 0000000B.00000000.293269223.0000000001208000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 0000000B.00000003.324153787.000000007F8D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000B.00000003.315153554.000000007DEF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000B.00000003.320355698.000000007EED0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000B.00000003.309591822.000000007CF10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000B.00000002.517622759.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000B.00000000.288998400.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 6308 Parent PID: 7128

General

Start time:	20:08:00
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0xdf0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 4088 Parent PID: 6308

General

Start time:	20:08:01
Start date:	30/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net.exe PID: 6836 Parent PID: 6308

General

Start time:	20:08:07
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\net.exe
Wow64 process (32bit):	true
Commandline:	net user /domain
Imagebase:	0x330000
File size:	46592 bytes
MD5 hash:	DD0561156F62BC1958CE0E370B23711B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: net1.exe PID: 6436 Parent PID: 6836

General

Start time:	20:08:07
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\net1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\net1 user /domain
Imagebase:	0x1a0000
File size:	141312 bytes
MD5 hash:	B5A26C2BF17222E86B91D26F1247AF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis