ID: 438548
Cookbook: browseurl.jbs
Time: 18:27:47
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

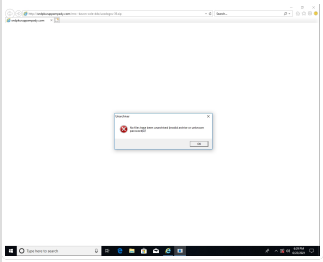
Windows Analysis Report http://sndpkuruppampady.co…

Overview

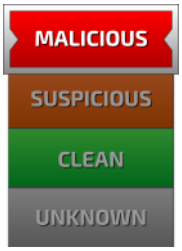
General Information

Sample URL:	http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip
Analysis ID:	438548
Infos:	

Most interesting Screenshot:



Detection

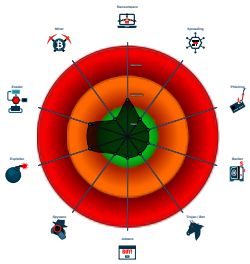


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e.…
- Creates a process in suspended mo…
- Detected potential crypto function
- Found inlined nop instructions (likely…
- Potential browser exploit detected (p…
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 900 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5340 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:900 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - unarchiver.exe (PID: 6004 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip' MD5: DB55139D9DD29F24AE8EA8F0E5606901)
    - 7za.exe (PID: 3124 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\5g3nu0sr.qil' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 4256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

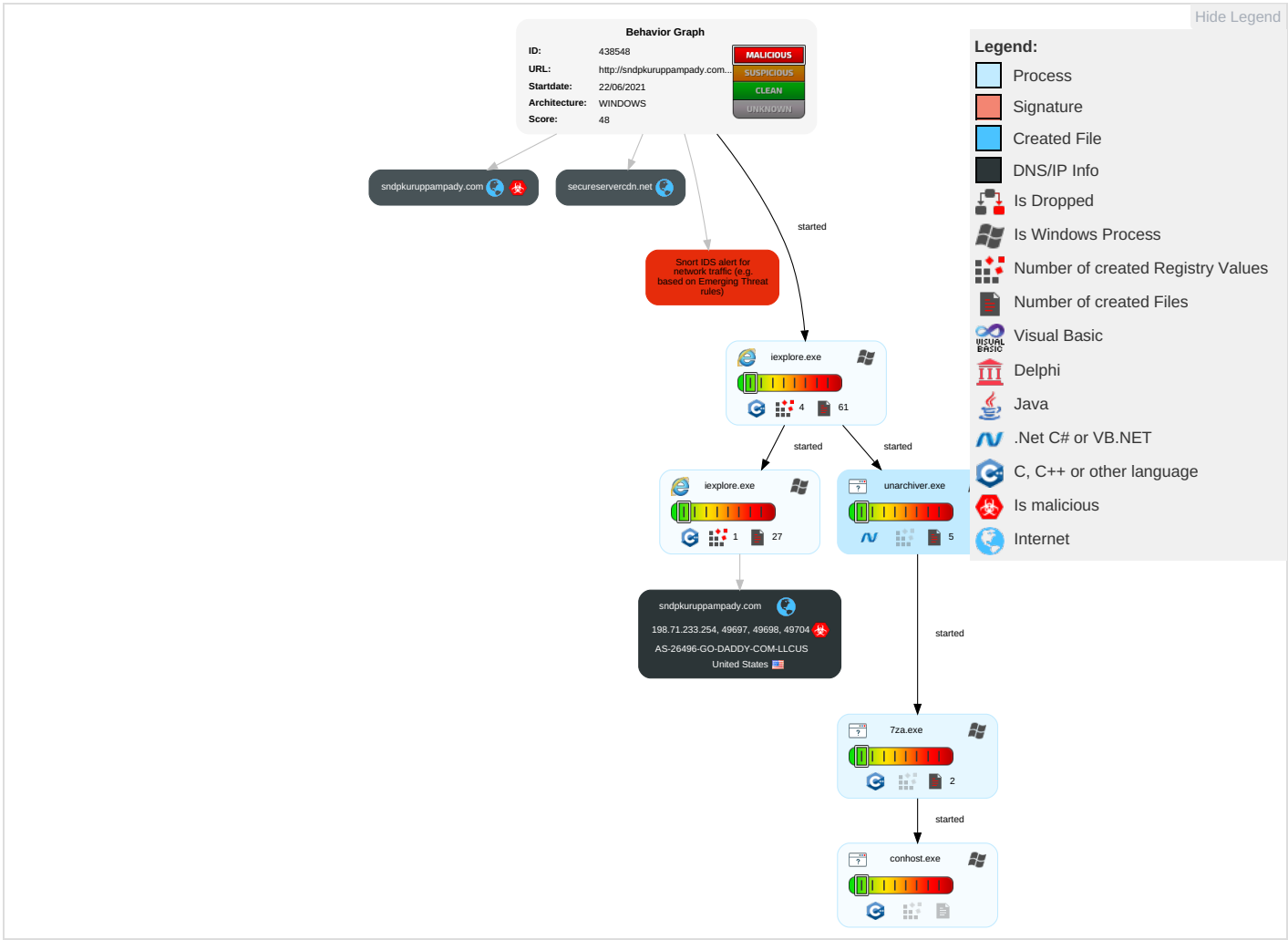
Networking:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Exploitation for Client Execution 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap		Carri Billin Fraud

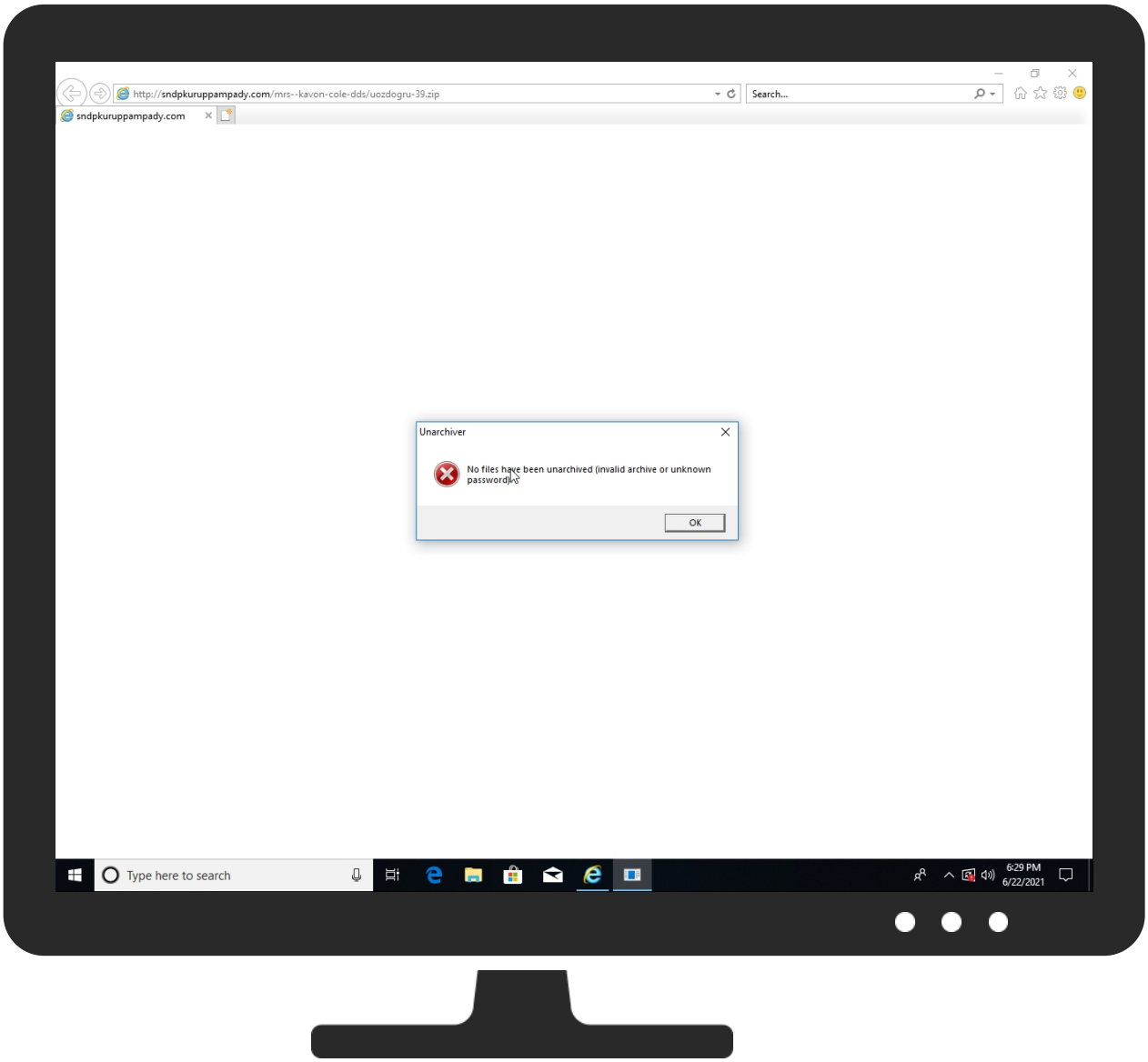
Behavior Graph



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
http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://sndpkuruppampady.com/favicon.ico	0%	Avira URL Cloud	safe	
http://sndpkuruppampady.com/mrs--kavon-cole-dds/documents.zip	0%	Avira URL Cloud	safe	
http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zipRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sndpkuruppampady.com	198.71.233.254	true	true		unknown
secureservercdn.net	192.124.249.16	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip	true		unknown
http://sndpkuruppampady.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip	true		unknown
http://sndpkuruppampady.com/mrs--kavon-cole-dds/documents.zip	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.71.233.254	sndpkuruppampady.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438548
Start date:	22.06.2021
Start time:	18:27:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip
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:	15
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@8/13@3/1
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{56FCBAF3-D3C2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.88098787947482
Encrypted:	false
SSDEEP:	96:roZfZn2OWWt/bfP5Q3KMxvquN1QBxfzQ+6rM20:roZfZn2OWWtjfP5RMUukHfzcrC
MD5:	22ABC3C72A616E863C27E52B33983F35
SHA1:	F8C13054EF4992B4D7D9052F57BBDCDBD1B5558A
SHA-256:	48C31B73D8F572FF261CB64D671D9F3F2C9DC0C8370487951956EA4FFC821CE8
SHA-512:	F5A2B78D55666E7B77484544714BCD3E678F48279DB98AE7F318B70037414BEFD7BC2BFE2320A328E25276F4334B3D8E5B2F5113E97BC82DD3B3797E18196E8E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{56FCBAF3-D3C2-11EB-90E5-ECF4BB570DC9}.dat	
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{56FCBAF5-D3C2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24236
Entropy (8bit):	1.643178287668459
Encrypted:	false
SSDEEP:	48:IwUGcprhGwpaZG4pQhGrapbSFGQpBiGHHpc/TGUp8wGzYpmkbGopumuJwGeNpm:rIZ7Q76xBSvj52JWEMgP5g
MD5:	C4ECAF324512D86A9713BA1B46117052
SHA1:	97314CA490F10F08CDE2CC1C46F55679140F9598
SHA-256:	6183FC57FD5EBF9D196E5957EBCD1EC5AE0CDC61804EFC319DB9377BFAD8D774
SHA-512:	45674CC0369A25DB9F81F84E6CF53A4BDB6A7FCB11C9893BB4419E687B035F492EFE33AE5443E9DECCB47EE515990A3687055F3AAF78766316AA0FC815487A7
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{60E0A826-D3C2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563531453955824
Encrypted:	false
SSDEEP:	48:Iw0GcprBGwpasG4pQcGrapbSEGQpKlG7HpRoTGIpG:roZbQs6aBScAUTsA
MD5:	D470B391862367CA01854BDFCA653388
SHA1:	376C563834ED8FFAAFDE73E041076B1EB6E8C842
SHA-256:	5FA3C602E0AEAE5CBC68883F93DBD9260E765074C46430EE99364A06D324B3F2
SHA-512:	05DC013095B14C4DF601B62697BB81C903A7B85C0A16756B69CD556F980C76C9ED1B08A7CE05157B8FB786DE9127371F504AA616F1DC18E466AE1169A19B62C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\documents[1].zip	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	149509
Entropy (8bit):	**7.997825098415298**
Encrypted:	**true**
SSDEEP:	3072:A+tg9Y7pLYWe09fTZyCd1xXL2ylUBWC6CFve7bpCxAVIKo5I/19/K00b:5sPp0jyix72yliWC69sYo5YTg
MD5:	A06BE586FC172FFC8792768EF2932967
SHA1:	EED0A41AB898C548853F197661F71D7D303F958F
SHA-256:	F154F4BBB7901063AC70641DED71FB6A788040FC69B386AA390B3299CAD9BC2E
SHA-512:	08C78202FF0EEB9F1139C36A2EEE2F6F6F653BA1F63A21DE0789E4DF0A500508DDB85C38AC0877BB4DBEC5A0007D4090266DE70D58CCB3D3320C198C2C10D6 1
Malicious:	false
Reputation:	low
Preview:	PK.....^.Ry^..YG..6o.....aim-1276697785.xlsb.Z.w....gf....3.....s...1C..bfzff;1&f.....V.....Z.p.H{..H...IOE.....r.....%8..,.xH=q.{Ws{W#./Gs...O;[.<hH...H..o..[;....z...Dg.|.. ...)..3.....'.h..&...G....).ve8...i...3....'.....U[.|U...##.\Y...Cc....l.....d...{[.4.N...j.s.d..q.g.Q6\y.).-1.....;;.2...n...I..9.{4J...Z...a.*.c.-.q6.AF..L.2(..x.2...k..0..\t7....A.J..ye.....N. i....)*].k...Fy..6/..B.g....p[..{....'G8.....A.=._.,!.....&..hr_...'2.c../.XG._.G.R.B.V...F.....?.,Y..T..Z=x.y..C..9..)..D.z.A.E.56[..@IC..S..*`.T.[...F..jx....]Q...e.H<....cu.....YM.|..^Wt..... ..e..`.M....}....~.....r0..?-//`  ^_. .5M..o..Y.oY..-M.9.....b..z..Oe.....e.s.....b.Doo.hK....O/..G.J:.$.+..T.M....@g..Y.}...tq.|..~.M~._.H.:.U.q..../."To.T.z.4.%..s..s...._.E;.5|.... .TF&vG....*v.&...\-`.2..x.I9.dx...!..#..5e.....M..V.Eb...B....C.....T.^F.b...T!*.L..&-...O..2.6...r*.v;....e.pp.1qp.a1....2.....p{....C^...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\uozdogru-39[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.8569078590363395
Encrypted:	false
SSDEEP:	3:uMBabGMoGLI0QWK8HIuRZdaOFG4KRNdBiR20gJYRnd7CJMKD1HQBIXWec7DSn:d5MoGLmApb8OOBibDRd7Q1wBqWeYDSn
MD5:	92EBBA2D7B311C7246056BDCDB51D970
SHA1:	C5AEE2411EA71A95B180CDFB8B620CC3CA0FD391
SHA-256:	10FAEE96424F7E1B9A87C493A59F0A7ECF999B15FF6A2E9FFC386BC70E7042BD
SHA-512:	4A2B490A383BDEF1964D568B47FBA2F43CD07EA5DEE691E746AF35B189E21C8B3A1991AF1004DCAB85CEFA742510E0561A596F9EF808A033EEA23791B184494D
Malicious:	false
Reputation:	low
Preview:	<script>location.pathname = document.getElementById('ll').getAttribute('data-rr');</script>Wait...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip.5uu3uf1.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	149509
Entropy (8bit):	**7.997825098415298**
Encrypted:	**true**
SSDEEP:	3072:A+tg9Y7pLYWe09fTZyCd1xXL2ylUBWC6CFve7bpCxAVIKo5I/19/K00b:5sPp0jyix72yliWC69sYo5YTg
MD5:	A06BE586FC172FFC8792768EF2932967
SHA1:	EED0A41AB898C548853F197661F71D7D303F958F
SHA-256:	F154F4BBB7901063AC70641DED71FB6A788040FC69B386AA390B3299CAD9BC2E
SHA-512:	08C78202FF0EEB9F1139C36A2EEE2F6F6F653BA1F63A21DE0789E4DF0A500508DDB85C38AC0877BB4DBEC5A0007D4090266DE70D58CCB3D3320C198C2C10D61
Malicious:	false
Reputation:	low
Preview:	PK.....^.Ry^..YG..6o.....aim-1276697785.xlsb.Z.w....gf....3.....s...1C..bfzff;1&f.....V.....Z.p.H{..H...IOE.....r.....%8..,.xH=q.{Ws{W#./Gs...O;[.<hH...H..o..[;....z...Dg.|.. ...)..3.....'.h..&...G....).ve8...i...3....'.....U[.|U...##.\Y...Cc....l.....d...{[.4.N...j.s.d..q.g.Q6\y.).-1.....;;.2...n...I..9.{4J...Z...a.*.c.-.q6.AF..L.2(..x.2...k..0..\t7....A.J..ye.....N. i....)*].k...Fy..6/..B.g....p[..{....'G8.....A.=._.,!.....&..hr_...'2.c../.XG._.G.R.B.V...F.....?.,Y..T..Z=x.y..C..9..)..D.z.A.E.56[..@IC..S..*`.T.[...F..jx....]Q...e.H<....cu.....YM.|..^Wt..... ..e..`.M....}....~.....r0..?-//` ^_. .5M..o..Y.oY..-M.9.....b..z..Oe.....e.s.....b.Doo.hK....O/..G.J:.$.+..T.M....@g..Y.}...tq.|..~.M~._.H.:.U.q..../."To.T.z.4.%..s..s...._.E;.5|.... .TF&vG....*v.&...\-`.2..x.I9.dx...!..#..5e.....M..V.Eb...B....C.....T.^F.b...T!*.L..&-...O..2.6...r*.v;....e.pp.1qp.a1....2.....p{....C^...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip.5uu3uf1.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip:Zone.Identifier	
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D12799027241450980651994501423A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low
Preview:	3

C:\Users\user\AppData\Local\Temp\5g3nu0sr.qil\aim-1276697785.xlsb	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	159542
Entropy (8bit):	7.96115135206652
Encrypted:	false
SSDEEP:	3072:aIIh9vajtC1gBbZmxVymd1xXPMU9VlUBWA6CFvA7bRCxAVIKPMI2:ZIQegBbcxVyWxfMU3liWA6FsYP+
MD5:	1019BFEBB97DE3EB8EC428358587BEF1
SHA1:	964A23BBB0CE3021464518510F1E3DF3FEF20BC9
SHA-256:	2FE2BABFCC7EA5AD682D772D74AEE8D1CDBD6E1974274669B262D9A6D4C8AAA3
SHA-512:	E1B0D59BD7E3B75B119EF4CFEA96C75B73CFC6854FE1CDF2FD06E605D86B310578732F0A8D7B8312CF32B2A3B7A11B3219E58EB5C95E2507AC2BAA72CE64D46C
Malicious:	false
Reputation:	low
Preview:	PK.....!.....[Content_Types].xml ...(..... ....U.N.0..W.?D.....,....$.z6....-{...3..m.v.F..$q.....{q..x.....+..Ni.....++"J..q.*.....?-.6.bAh.+. .oB..VF.<X..r..H..^..r..t6."jg.,..8.rq.+.h.....6.{mY.}._. .....Z".*...m,..... '.....:..+.../.X.^~o..~.....&. ...].9sB.c.}<!c.(./.s.q.T....72.O.3.3...ID..6O....qp.N../....*.&....~...\.>.m.L.&....)..~.../...).$....4. .u...55.`..j.kP.~li.y.y...].qc N.k...zld.u....i... G.<1#.[@L.b.>fd..>.Ty0Z...#.. .sD...K...S.

C:\Users\user\AppData\Local\Temp\pcdulxpe.xs1\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1468
Entropy (8bit):	5.1591523526521845
Encrypted:	false
SSDEEP:	24:Oc2ceYeVY2RQw20iJG20iJjWIG20iJG20iJUw020iJfFv20iJG20iJFTAYeVY20l:OcPeDi6QwNGGNGbGNGGNGp0NGBNGGNGT
MD5:	1D1E795E7B8332A2A02BB10EE5863E2F
SHA1:	9C0B3819828C0C4DC790837DE36539E5DD1307D1
SHA-256:	0C1F22654C6E920D6D20A758375A6D82F723529647D725E4776D83AA00653308
SHA-512:	8DAE34F7293938A155383A7AC25791FFDE4A4521ECBB417591FED28886FC31C7CF41532747413FB9049285935C1FB7766F58C43C8CF08FF29E2FC9302FDFAAE7
Malicious:	false
Reputation:	low
Preview:	06/22/2021 6:29 PM: Unpack: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip..06/22/2021 6:29 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\5g3nu0sr.qil..06/22/2021 6:29 PM: Received from standard out: ..06/22/2021 6:29 PM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..06/22/2021 6:29 PM: Received from standard out: ..06/22/2021 6:29 PM: Received from standard out: Scanning the drive for archives:..06/22/2021 6:29 PM: Received from standard out: 1 file, 149509 bytes (147 KiB)..06/22/2021 6:29 PM: Received from standard out: ..06/22/2021 6:29 PM: Received from standard out: Extracting archive: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip..06/22/2021 6:29 PM: Received from standard out: --..06/22/2021 6:29 PM: Received from standard out: Path = C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip..06/22/2021 6:29 PM: Received from

C:\Users\user\AppData\Local\Temp\~DF426483966D72EDC8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5157573192245184
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lobI9lobY9lWbBE3Kc6fS5KW:kBqoIHhQKZ6IW
MD5:	F5581A4325C6CB9B0440BF9FDE11AA76
SHA1:	56A1B38E731F00BFDDDA9F834CE8984190A253D9
SHA-256:	35B24AB08E34E7810B3B27BEA1B2B00D8B2665538692F9674962AF8EB0DF12AD
SHA-512:	BFDDF470CBC952B008605F6565485FB8FD93C1D13D023126BC08BABCC2854AED5A1FD9A2DB2A6CDACC6F78304DF3E54A715BD9E363C9790B145D1AAC74AF08F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF426483966D72EDC8.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4EEC81F457CBDB58.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34429
Entropy (8bit):	0.36247696279437985
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwy9lwC9l209l2U9l/kO:kBqoxKAuvScS+1bZIkIkYmuJP
MD5:	C7B69592A6E5CF50B6CF0A44CE20A99A
SHA1:	35C7C4F29AA8B9123E235766278A6192B2074443
SHA-256:	0F19A6DD30789DEFBC844CAC28BB7D33F00919A861B38EF90686CDBE6A7A86BC
SHA-512:	8129CD88BB82F39D3CC39A3456EC86FAA3E74AE599FF9657604BAD07743C2B3D6E196B712F124A4A3D1B827F7E98478C8AEB67CFD15FE9F193FD7C28B55977C 9
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFED12FFEC4428B97E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.33703736285108915
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAYvZYqs98dd:kBqoxxJhHWSVSEabYvZYn9cP1
MD5:	6FD8B5F5A01D5F25D1A40CDAB8C19316
SHA1:	F73606C068013D879C1569110EE17DCB90500245
SHA-256:	B4686C86CCCAF7551E6BF5E432B6C993BBAC37AD368A00E0E4028D7628173621
SHA-512:	26A530D712A491F37890D763449DE86ADCF6BB77998A4A1DFC245CE43D9848535A51AB7AA0CD161079D7C9F8C2753E145DD7A68F5AF891CA7F82C6F43CE5C7
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:28:43.800333	TCP	3134	WEB-CLIENT PNG large colour depth download attempt	80	49698	198.71.233.254	192.168.2.5
06/22/21-18:28:43.800333	TCP	3133	WEB-CLIENT PNG large image height download attempt	80	49698	198.71.233.254	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:28:42.651504040 CEST	192.168.2.5	8.8.8.8	0x7a2d	Standard query (0)	sndpkurupp ampady.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:29:44.068449020 CEST	192.168.2.5	8.8.8.8	0x9962	Standard query (0)	sndpkurupp ampady.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:29:44.435430050 CEST	192.168.2.5	8.8.8.8	0xbf05	Standard query (0)	secureserv ercdn.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:28:42.724716902 CEST	8.8.8.8	192.168.2.5	0x7a2d	No error (0)	sndpkurupp ampady.com		198.71.233.254	A (IP address)	IN (0x0001)
Jun 22, 2021 18:29:44.127366066 CEST	8.8.8.8	192.168.2.5	0x9962	No error (0)	sndpkurupp ampady.com		198.71.233.254	A (IP address)	IN (0x0001)
Jun 22, 2021 18:29:44.499984980 CEST	8.8.8.8	192.168.2.5	0xbf05	No error (0)	secureserv ercdn.net		192.124.249.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sndpkuruppampady.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49698	198.71.233.254	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:28:42.868660927 CEST	307	OUT	GET /mrs--kavon-cole-dds/uozdogru-39.zip HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: sndpkuruppampady.com Connection: Keep-Alive
Jun 22, 2021 18:28:43.005182981 CEST	308	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Age: 1495 Cache-Control: no-store, no-cache, must-revalidate Content-Encoding: gzip Content-Length: 150 Content-Type: text/html; charset=UTF-8 Date: Tue, 22 Jun 2021 16:03:46 GMT Expires: Thu, 19 Nov 1981 08:52:00 GMT Pragma: no-cache Vary: Accept-Encoding X-Backend: local X-Cache: cached X-Cache-Hit: HIT X-Cacheable: YES X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Data Raw: 1f 8b 08 00 00 00 00 00 00 03 35 8d 41 0a c2 30 10 45 af 12 b2 49 bb 48 72 00 d3 82 82 8b 9e c0 f5 98 09 3a 38 4d 4a 32 2d e8 e9 b5 50 77 8f 0f ef bf 80 b4 29 c2 41 33 6b 85 20 60 6b 1d b4 9f 6b b3 f6 05 5b c9 36 16 4e 16 b1 79 2c 71 9d 53 96 e6 3e b4 e8 31 f8 9f 3a 86 16 2b 2d 32 72 89 20 54 b2 5b 40 9e 19 e6 a4 06 f5 17 dc 23 c9 95 d3 8e 97 f7 84 9d 61 36 fd 3e 9e 45 2a dd 57 49 9d 39 d2 a6 3f 05 7f 5c de 80 c4 39 f7 05 0e 83 a9 28 a2 00 00 00 Data Ascii: 5A0EIHr:8MJ2-Pw)A3k `kk[6Ny,qS>1:+-2r T[@#a6>E*WI9?\9(

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:28:43.271178007 CEST	313	OUT	GET /mrs--kavon-cole-dds/documents.zip HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: http://sndpkuruppampady.com/mrs--kavon-cole-dds/uozdogru-39.zip Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: sndpkuruppampady.com Connection: Keep-Alive
Jun 22, 2021 18:28:43.404979944 CEST	317	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Age: 429595 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Description: File Transfer Content-Disposition: attachment; filename= Content-Length: 149509 Content-Transfer-Encoding: binary Content-Type: application/octet-stream Date: Thu, 17 Jun 2021 17:08:46 GMT Expires: 0 Pragma: public X-Backend: local X-Cache: cached X-Cache-Hit: HIT X-Cacheable: YES X-Content-Type-Options: nosniff X-Xss-Protection: 1; mode=block Data Raw: 50 4b 03 04 14 00 00 00 08 00 ec 5e d1 52 79 5e b6 d1 59 47 02 00 36 6f 02 00 13 00 00 00 61 69 6d 2d 31 32 37 36 36 39 37 37 38 35 2e 78 6c 73 62 ec 5a f5 77 dd cc 11 f5 67 66 c6 98 99 99 e1 33 c4 cc f8 cc 10 73 cc cc 0c 31 43 e2 18 62 66 7a 66 66 3b 31 26 66 86 98 99 99 b9 56 e1 f4 b4 a7 fd 0b 5a fd 70 df 48 7b ef ec 48 bb 9a 1d 49 4f 45 1e 0a 1a 1b 02 16 02 1e 02 02 82 1c 82 a4 72 a2 eb e4 0f 08 88 25 38 08 08 2c 08 78 48 3d 71 07 7b 57 73 7b 57 23 0d 2f 47 73 17 03 16 4f 3b 5b b2 3c 68 48 ba 1c 08 48 88 ff 6f ff d3 5b 3b e8 87 d2 12 1b 7a 87 d6 81 88 44 67 de 7c 1b 11 18 fc 9b 29 1c 12 33 1c 97 aa c4 9b e7 fc a8 bf bb 86 d9 27 f0 68 95 f3 26 cc 2e d2 bd 47 aa a4 83 ca 29 e1 76 65 38 9d c0 c7 69 b6 a1 c8 33 18 bd a1 0e 27 fd 92 80 f1 fb ac 92 55 5b e5 7c 55 db d0 05 23 23 85 5c 59 81 13 2e 43 63 d0 cf d1 e4 6c 11 e6 13 1e 12 13 b1 8f 84 8c b3 64 0f 0e ef 7b 5b 83 34 a5 4e 84 b4 1f 6a 9d 73 93 64 86 aa 71 0d 67 d1 9c 51 36 5c 79 1e 29 ac 2d 31 98 92 bf f1 cd 3b 3b a1 32 de 7f ac 6e de db bb e6 49 f0 b1 d3 39 f7 7b 34 4a 00 7f bb 5a d9 d3 a5 80 61 c8 2a df b0 63 ca 2d fb 71 36 0f 41 46 1b 88 4c b8 32 28 d0 8c c4 78 8a 32 ce 9a a0 dd 6b e8 ef 30 07 e5 bf 5c 74 37 f9 f8 1c 01 41 83 4a d6 f3 79 65 c7 e0 86 df e5 fd 4e b5 69 be 9f 10 b9 29 2a 5d 01 6b b8 cb 89 d3 9c 46 79 0e 0e 36 2f c7 9a f2 42 02 67 1e e7 c6 c2 a7 70 5b 09 ec 7b 1e e5 b0 98 ea 0e 27 47 38 a5 a0 0e d6 ea 86 87 41 86 3d 9a 5f e8 2c 21 fe 03 18 99 fa df 85 b1 ec 26 14 c6 68 72 5f aa 89 e8 af 27 32 fc 63 b6 eb 2f 9b 58 47 f7 5f e9 47 a9 52 f3 a3 42 b8 56 c9 2e dc 46 07 16 b9 b9 e7 3f 90 2c 59 17 da a8 54 fa db 5a 3d 78 15 79 11 87 43 19 e0 39 99 92 29 d5 d8 44 e3 97 7a db 9a 41 b8 45 07 35 36 5b 0d 07 40 49 43 0b b1 53 86 ea 89 2a 60 9a 54 0b 5b 98 f5 c7 46 0b 07 6a 78 b1 e9 f6 c0 5d 51 06 95 92 65 bb 48 3c f7 0c c8 cf 63 75 a8 f7 8a 85 8a 8b c7 59 4d 05 7c 80 bf 5e 57 74 14 9e b4 c2 fe e0 cd d9 65 7f 82 60 e0 4d 11 1c f8 ce 7d f1 b1 d3 7f 85 7e b2 85 dd c0 91 ed cf cf a3 72 30 d6 f1 8d 3f 2d 2f 2f 60 20 20 5e 5f a1 20 fe 35 4d 88 07 6f f6 dd be 59 0a 6f 59 00 e9 2d 4d 18 39 9b db ba b0 b2 00 f8 ff f4 f0 ff 0d d8 62 12 c6 94 7a d8 90 fb 4f 65 da c5 b7 1e 0f ec 65 e0 73 1b da c8 0a 96 d1 19 d0 d6 a8 ed 09 1b 62 f3 a9 44 6f 6f cc 68 4b b8 1a 89 9f 4f 2f c7 b2 db 97 47 a6 4a 3a f9 24 18 2b 83 dd 54 83 4d 8a fb b4 e7 40 67 13 ed 95 59 a2 7d 12 a3 e3 74 71 8c 7c ce a1 06 7e 01 4d 7e bb 5f d4 48 a2 3a ae 55 cd 71 f0 18 f7 d4 2f c6 22 54 6f 85 54 99 7a eb 86 92 34 bb 25 e8 Data Ascii: PK^Ry^YG6oaim-1276697785.xlsbZwgf3s1Cbfzff;1&fVZpH{HIOEr%8,xH=q{Ws{W#/GsO;[<hHHo[;zDg|)3 'h&.G)ve8i3'U[|U##\Y.Ccld{[4NjsdqgQ6\y)-1;;2nI9{4JZa*c-q6AFL2(x2k0\t7AJyeNi)*]kFy6/Bgp[{'G8A=_,!&hr_'2c/XG_GRB V.F?,YTZ=xyC9)DzAE56[@ICS*`T[Fjx]QeH<cuYM|^Wte`M}~r0?-//` ^_ 5MoYoY-M9bzOeesbDoohKO/GJ:$+TM@gY}tq|~ M~_H:Uq/"ToTz4%

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49704	198.71.233.254	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:29:44.268506050 CEST	499	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: sndpkuruppampady.com
Jun 22, 2021 18:29:44.405162096 CEST	500	IN	HTTP/1.1 302 Found Age: 444526 Content-Length: 0 Content-Type: text/html; charset=UTF-8 Date: Thu, 17 Jun 2021 13:00:56 GMT Location: https://secureservercdn.net/198.71.233.254/m8l.34d.myftpupload.com/wp-content/uploads/2020/03/cropped-GuruSquar-32x32.png X-Backend: local X-Cache: cached X-Cache-Hit: HIT X-Cacheable: YES X-Content-Type-Options: nosniff X-Redirect-By: WordPress X-Xss-Protection: 1; mode=block

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 900 Parent PID: 792

General

Start time:	18:28:40
Start date:	22/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7bd500000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: iexplore.exe PID: 5340 Parent PID: 900

General

Start time:	18:28:41
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:900 CREDAT:17410 /prefetch:2
Imagebase:	0x1330000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: unarchiver.exe PID: 6004 Parent PID: 900

General

Start time:	18:29:21
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip'
Imagebase:	0x580000
File size:	10240 bytes
MD5 hash:	DB55139D9DD29F24AE8EA8F0E5606901
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 7za.exe PID: 3124 Parent PID: 6004

General

Start time:	18:29:22
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\5g3nu0sr.qil' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\documents.zip'
Imagebase:	0xfc0000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4256 Parent PID: 3124

General

Start time:	18:29:22
Start date:	22/06/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis