ID: 562452
Sample Name: Sat#U0131nalma Sipari#U015fi - AR95647,pdf.scr
Cookbook: default.jbs
Time: 22:09:51
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

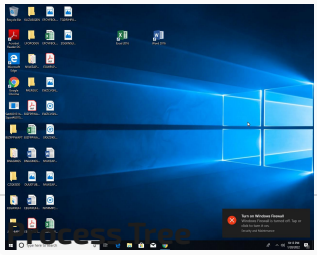
Windows Analysis Report

Sat#U0131nalma Sipari#U015fi -AR95647,pdf.scr

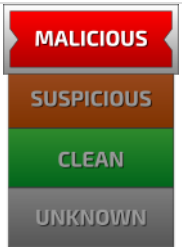
Overview

General Information

Sample Name:	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.scr (renamed file extension from scr to exe)
Analysis ID:	562452
MD5:	43c383d252b338..
SHA1:	9bff9ef837f3b17…
SHA256:	fa51b3b1d130a5..
Tags:	AgentTesla exe geo scr TUR
Infos:	



Detection



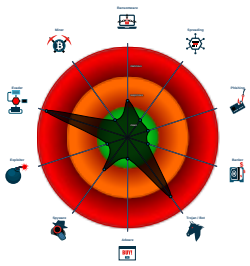
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe (PID: 6984 cmdline: "C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe" MD5: 43C383D252B3385D4EAA21E4ECCBF244)
  - Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe (PID: 6844 cmdline: C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe MD5: 43C383D252B3385D4EAA21E4ECCBF244)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Http",
  "HTTP method": "Post",
  "Post URL": "https://agusanplantation.com/udo/udo/inc/0315179f2c9558.php",
  "User Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.368811093.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.368811093.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.370441082.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.370441082.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.381669718.0000000002769000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30db1:$s1: get_kbok • 0x316e5:$s2: get_CHoo • 0x32340:$s3: set_passwordIsSet • 0x30bb5:$s4: get_enableLog • 0x3525f:$s8: torbrowser • 0x33c3b:$s10: logins • 0x335b3:$s11: credential • 0x2ff9d:$g1: get_Clipboard • 0x2ffab:$g2: get_Keyboard • 0x2ffb8:$g3: get_Password • 0x31593:$g4: get_CtrlKeyDown • 0x315a3:$g5: get_ShiftKeyDown • 0x315b4:$g6: get_AltKeyDown
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 29 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

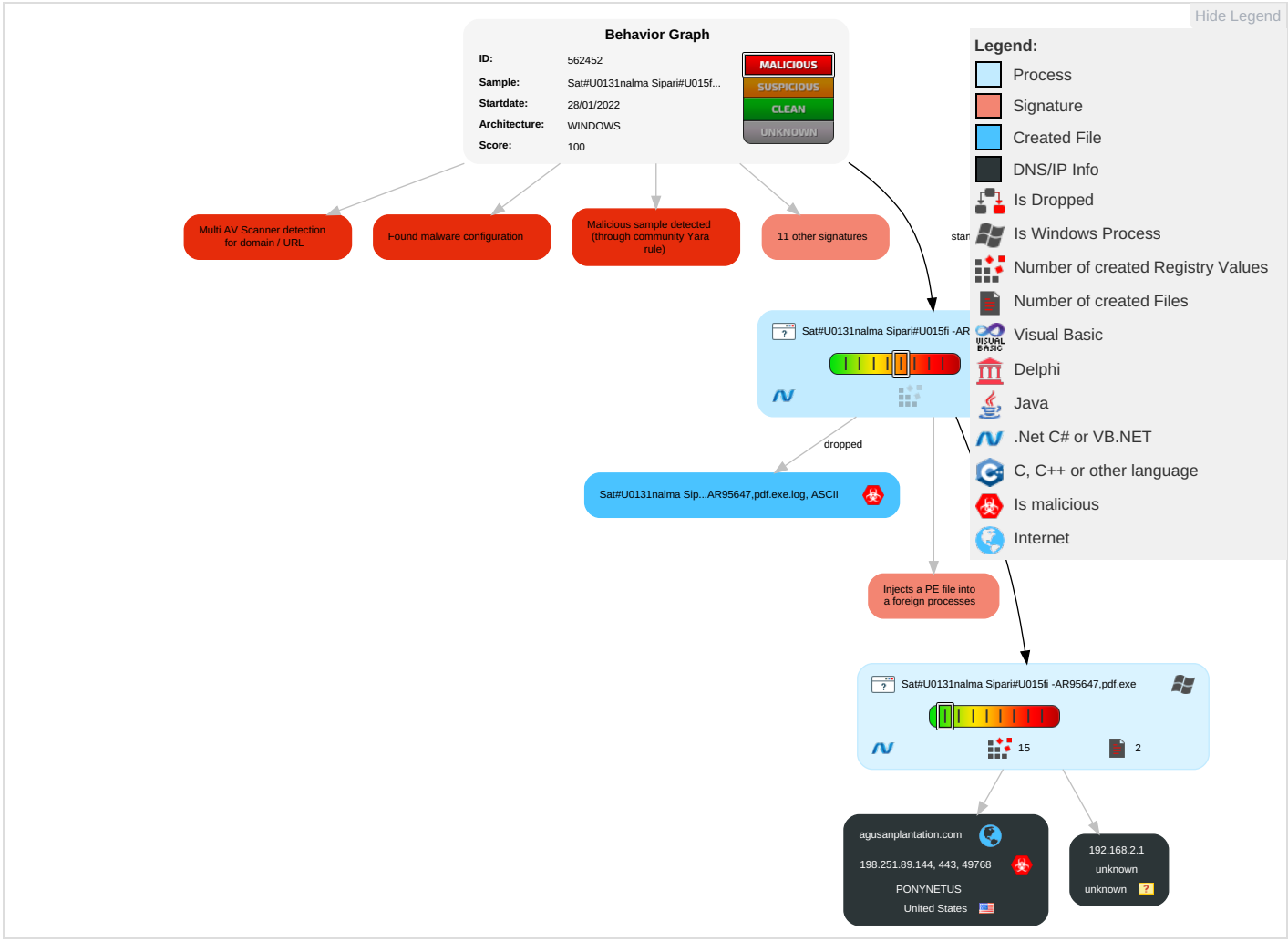
Remote Access Functionality

Yara detected AgentTesla

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 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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	1 Obfuscated Files or Information	Cached Domain Credentials	1 1 3 System Information 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	2 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

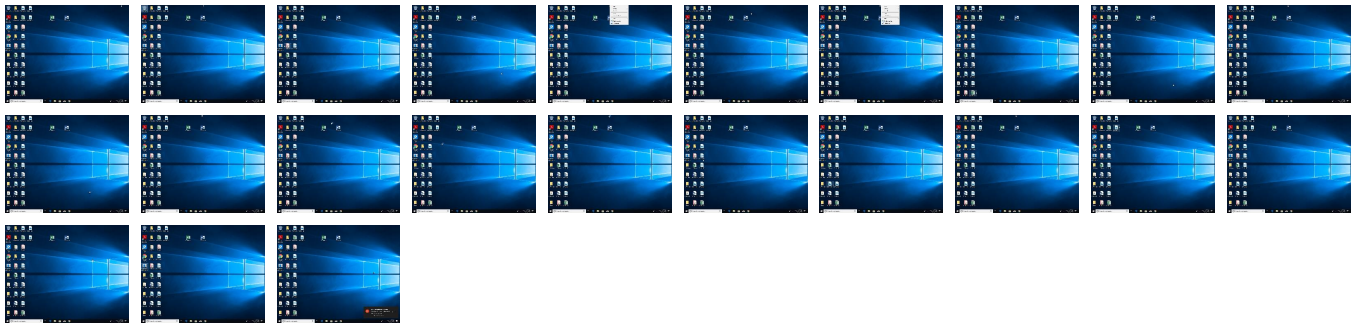
Behavior Graph



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
Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe	35%	Virustotal		Browse
Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.DarkStealerLoader	
Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
agusanplantation.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://blog.iandreev.com/	0%	Virustotal		Browse
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://agusanplantation.com4	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://ZzSQGD.com	0%	Avira URL Cloud	safe	
http://agusanplantation.com	100%	Avira URL Cloud	malware	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://agusanplantation.com	100%	Avira URL Cloud	malware	
http://https://agusanplantation.com/udo/udo/inc/0315179f2c9558.php127.0.0.1POST	100%	Avira URL Cloud	malware	
http://https://agusanplantation.com/udo/udo/inc/0315179f2c9558.php	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
agusanplantation.com	198.251.89.144	true	true	• 11%, Virustotal, Browse	unknown

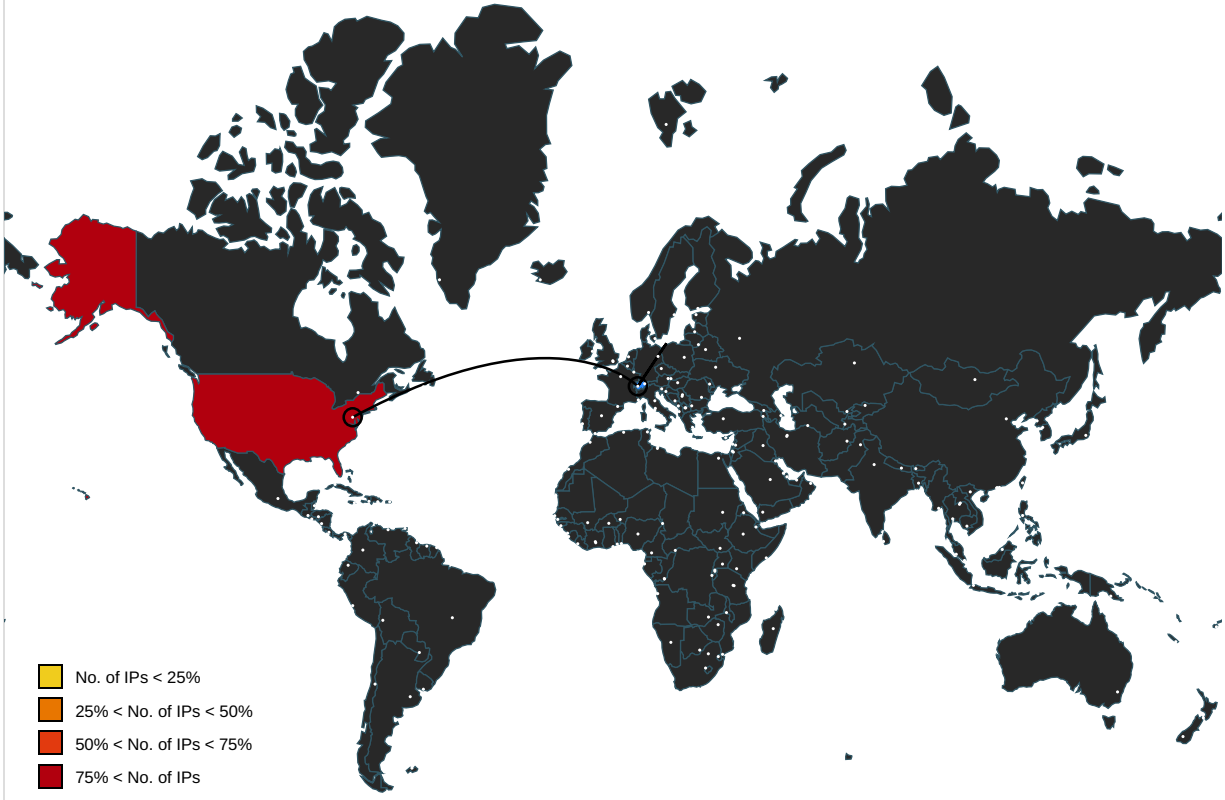
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000003091000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000000309100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://blog.iandreev.com/	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.381542855.00000000026B100 0.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://agusanplantation.com4	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568858553.000000000313800 0.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000000309100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.381542855.00000000026B100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ZzSQGD.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000000309100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://agusanplantation.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568890784.000000000315600 0.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.carterandcone.coml	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://agusanplantation.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568858553.000000000313800 0.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://agusanplantation.com/udo/udo/inc/0315179f2c9558.php127.0.0.1POST	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000000309100 0.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://agusanplantation.com/udo/udo/inc/0315179f2c9558.php	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568858553.000000000313800 0.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568744346.000000000309100 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000002.568858553.000000000313800 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.384224185.000000000678200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000001.00000002.382042190.00000000036B900 0.00000004.00000800.00020000.00000000.sdmp, Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe, 00000005.00000000.368811093.00000000004 02000.00000040.00000400.00020000.0000000 0.sdmp, Sat#U0131nalma Sipari#U015fi -AR 95647,pdf.exe, 00000005.00000000.3704410 82.0000000000402000.00000040.00000400.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.251.89.144	agusanplantation.com	United States		53667	PONYNETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562452
Start date:	28.01.2022
Start time:	22:09:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.scr (renamed file extension from scr to exe)
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:	20
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@3/1@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.7%) • Quality average: 56.2% • Quality standard deviation: 40.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 2.20.157.220
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:12:02	API Interceptor	425x Sleep call for process: Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.log

Process:	C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.597778252697803

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe
File size:	869376
MD5:	43c383d252b3385d4eaa21e4eccbf244
SHA1:	9bff9ef837f3b1742859b0ff14528c59ef87b0f0
SHA256:	fa51b3b1d130a540d92f8864a6daeb74b25a3b34306dd2d0d61e4a24c4ad5744
SHA512:	dedba6a609fc9143e837d59eff3179e80968f85db5e469ec330b64789c9be9d9725f7a3c63f22d3ac2cf0b7a93e433214e21a6b85a4e0b58026d17094aab247b
SSDEEP:	12288:qc7oo9xqQNl9qY4DeOxRRqu+bfYE8Q25GWVy1vw:qckovfNDqY4ykRRqujd3Gey
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....6.....T... ...`....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d54ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F3C3C0 [Fri Jan 28 10:21:52 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd54a0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd544e	0x1c	.text
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	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd34f4	0xd3600	False	0.522019145476	data	6.6031194739	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xd6000	0x1e8	0x200	False	0.861328125	data	6.62066080555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x5c0	0x600	False	0.427734375	data	4.11400581254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd80a0	0x334	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xd83d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

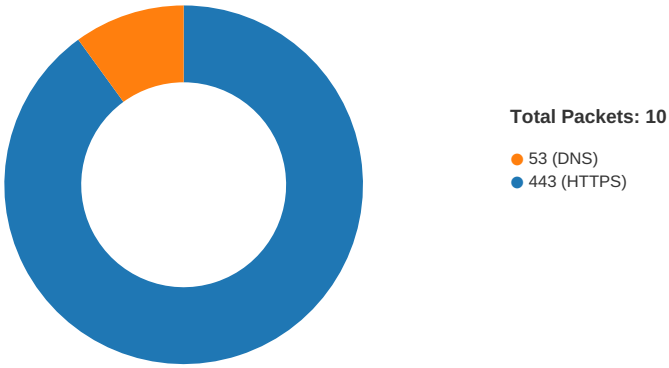
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	UnicodeDataHead.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	UnicodeDataHead.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:12:55.389868975 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:12:55.389926910 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:12:55.390032053 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:12:55.866844893 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:12:55.866872072 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:12:55.989129066 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:12:55.989315033 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:12:55.994330883 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:12:55.994343996 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:12:55.994638920 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:12:56.163947105 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:13:00.564177990 CET	49768	443	192.168.2.3	198.251.89.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:13:00.564737082 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:13:00.564790964 CET	443	49768	198.251.89.144	192.168.2.3
Jan 28, 2022 22:13:00.564837933 CET	49768	443	192.168.2.3	198.251.89.144
Jan 28, 2022 22:13:00.564867973 CET	49768	443	192.168.2.3	198.251.89.144

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:12:54.916333914 CET	60823	53	192.168.2.3	8.8.8.8
Jan 28, 2022 22:12:54.978343964 CET	53	60823	8.8.8.8	192.168.2.3

DNS Queries

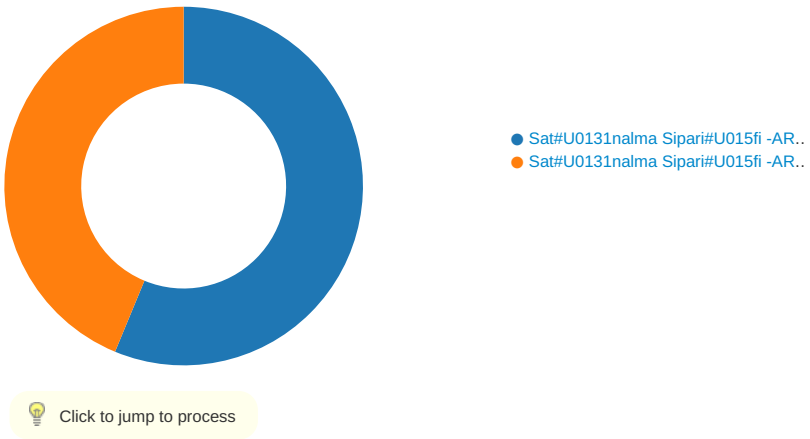
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:12:54.916333914 CET	192.168.2.3	8.8.8.8	0x38e3	Standard query (0)	agusanplantation.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 22:12:54.978343964 CET	8.8.8.8	192.168.2.3	0x38e3	No error (0)	agusanplantation.com		198.251.89.144	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe PID: **6984**, Parent PID: **3744**

General

Target ID:	1
Start time:	22:11:33
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe"
Imagebase:	0x1c0000
File size:	869376 bytes

MD5 hash:	43C383D252B3385D4EAA21E4ECCBF244
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.381669718.0000000002769000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.381542855.00000000026B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.382042190.00000000036B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.382042190.00000000036B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E74CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E74CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EA5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EA5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E725705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E72CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	69231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	69231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	69231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	69231B4F	ReadFile

Analysis Process: Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe PID: **6844**, Parent PID: **6984**

General

Target ID:	5
Start time:	22:12:04
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Sat#U0131nalma Sipari#U015fi -AR95647,pdf.exe
Imagebase:	0xcd0000
File size:	869376 bytes
MD5 hash:	43C383D252B3385D4EAA21E4ECCBF244
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.368811093.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.368811093.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.370441082.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.370441082.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.567660586.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.567660586.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.568744346.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.568744346.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000005.00000002.568744346.0000000003091000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.372540423.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.372540423.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.369389266.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.369389266.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E74CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E74CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E725705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E72CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E725705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	69231B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	69231B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly