ID: 743454
Sample Name: App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log
Cookbook: default.jbs
Time: 21:14:46
Date: 10/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

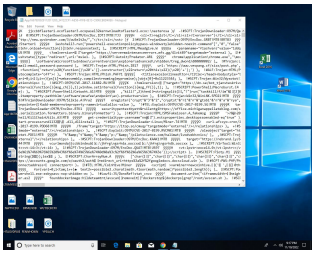
Windows Analysis Report

App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log

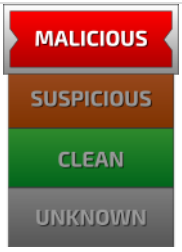
Overview

General Information

Sample Name:	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log
Analysis ID:	743454
MD5:	988e0cb19fbc2c…
SHA1:	1b091e30aa366a.
SHA256:	c289adee6ca95b..
Infos:	YARA



Detection



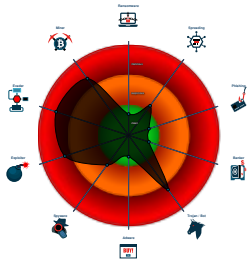
CobaltStrike, Follina CVE-2022-30190, Xmrig

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

Signatures

- Yara detected Powershell dedcode a…
- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Yara detected Microsoft Office Expl…
- Yara detected CobaltStrike Stager
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Yara detected AntiVM3
- Found strings related to Crypto-Mini…
- Found Tor onion address
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- notepad.exe (PID: 5416 cmdline: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x4724:$r1: p^o^w^e^r^s^h^e^l^l • 0x4724:$r2: p^o^w^e^r^s^h^e^l^l
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth	• 0x20dbf2:$s4: system.net.webclient).downloadfile("http • 0x8eb6:$s5: getstring([convert]::frombase64string(• 0x10c936:$s5: getstring([convert]::frombase64string(• 0x20328f:$s5: getstring([convert]::frombase64string(• 0x20cdf3:$s5: getstring([convert]::frombase64string(• 0x40e7d7:$s5: getstring([convert]::frombase64string(
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	PS_AMSI_Bypass	Detects PowerShell AMSI Bypass	Florian Roth	• 0x40a8b2:$s1: .getfield('amsicontext',[reflection.bindingflags]'nonpublic,static').
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Click to see the 6 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x8e88:$r1: p^o^w^e^r^s^h^e^l^l • 0x8e88:$r2: p^o^w^e^r^s^h^e^l^l
00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_PWSH_PasswordCredential_RetrievePassword	Detects PowerShell content designed to retrieve passwords from host	ditekSHen	• 0x81c9d4:$namespace: windows.security.credentials.passwordvault • 0x212ac8:$method1: retrieveall() • 0x212af8:$method2: .retrievepassword()
Process Memory Space: notepad.exe PID: 5416	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x37494a:$r1: p^o^w^e^r^s^h^e^l^l • 0x37494a:$r2: p^o^w^e^r^s^h^e^l^l
Click to see the 8 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Bitcoin Miner

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

Networking

Found Tor onion address

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion

Yara detected Powershell dedcode and execute

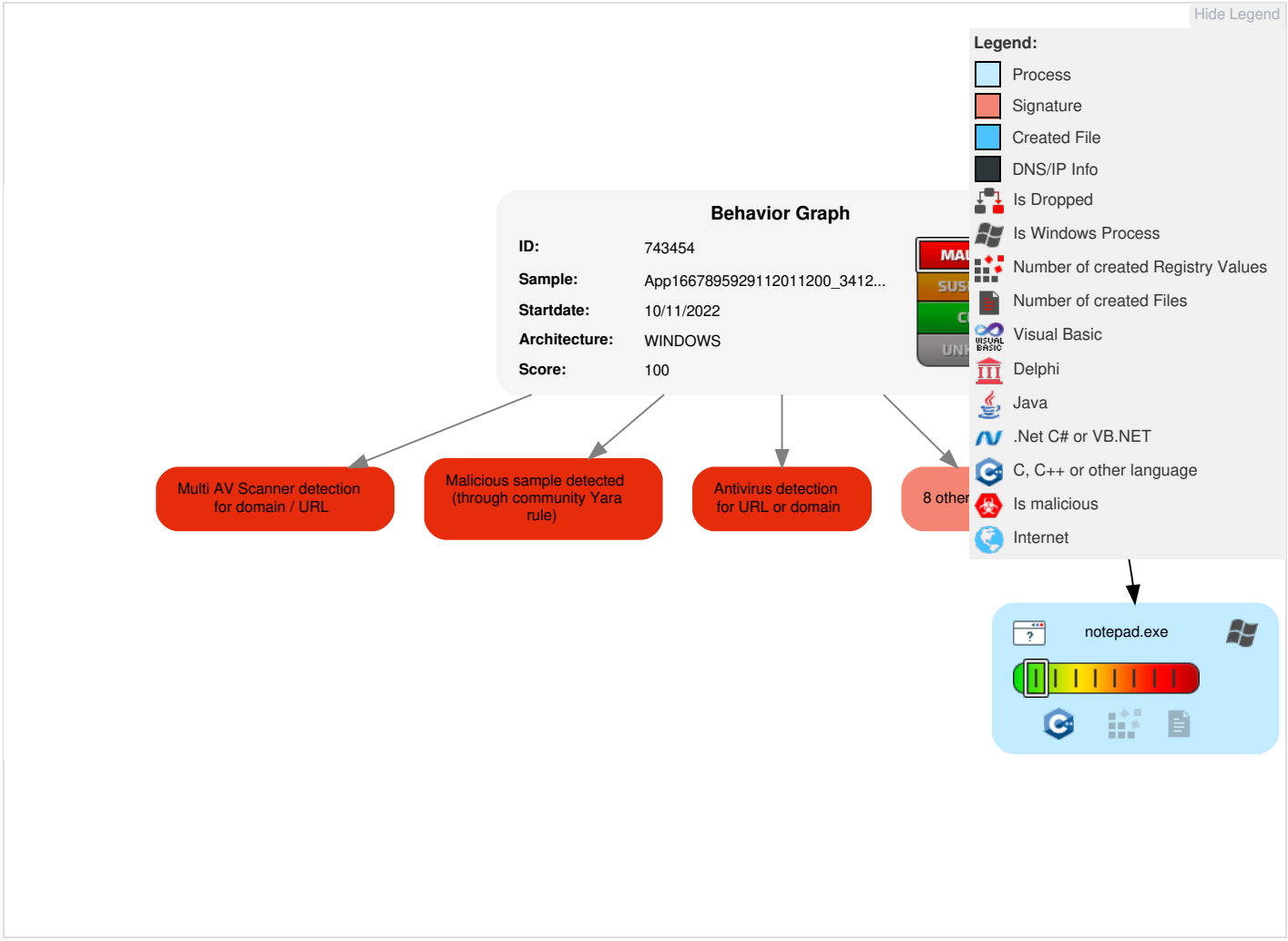
Remote Access Functionality

Yara detected CobaltStrike Stager

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
1 Replication Through Removable Media	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	1 Security Software Discovery	1 Replication Through Removable Media	Data from Local System	Exfiltration Over Other Network Medium	1 Proxy	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	Rootkit	LSASS Memory	1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

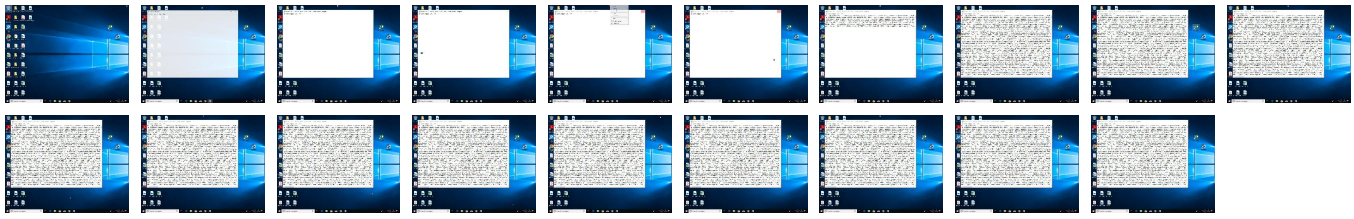
Behavior Graph

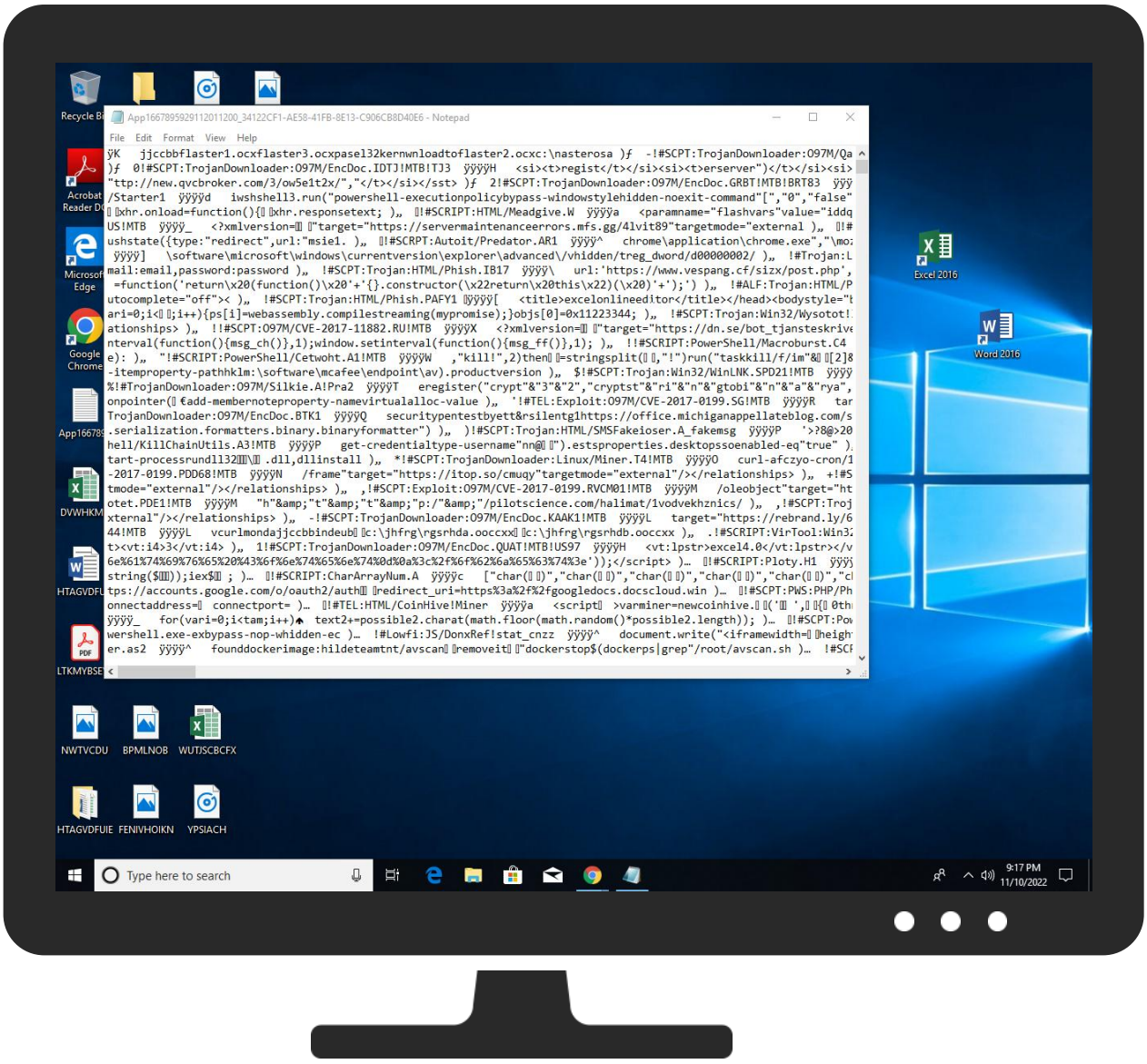


Screenshots

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
App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	16%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://spr-updates.ddns.net/spr_updates.php-o	0%	Avira URL Cloud	safe	
http://www.bonusesfound.ml/update/index.php	100%	Avira URL Cloud	malware	
http://https://gengengma.com/wp-content/uploads/vipe_11/send.php	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://doocument.m2diving.ml/fay/login.php?log	0%	Avira URL Cloud	safe	
http://www.bonusesfound.ml/update/index.php	10%	Virustotal		Browse
http://https://hitechceramics.com/egab/processor.php	0%	Avira URL Cloud	safe	
http://shgshgwsdynationalobjindustrialat18ygs.duckdns.org/receipt/invoice_202121.doc	100%	Avira URL Cloud	malware	
http://https://www.sputnikradio.net/radio/news/	100%	Avira URL Cloud	malware	
http://https://partoniroo.com/n9/u.js&&pingo0.org&&cd	0%	Avira URL Cloud	safe	
http://https://acaciavictorias.com/sxmal.php	0%	Avira URL Cloud	safe	
http://https://jovial-pasteur.159-89-118-202.plesk.page/wp-content/uploads/index.php	0%	Avira URL Cloud	safe	
http://https://diarnondfireplace.com/dobo/xxx.php?user=	0%	Avira URL Cloud	safe	
http://usa-national.info/gpu/band/grumble.dot	100%	Avira URL Cloud	malware	
http://https://tulsabailbondfinancing.com/dgImzmfueublehbmzi5jb20=	0%	Avira URL Cloud	safe	
http://192.210.240.8/doc_document/188.doc	100%	Avira URL Cloud	malware	
http://snapper.genesysindonesia.com/excel/excelz/index.php?email=	0%	Avira URL Cloud	safe	
http://https://gez.org.zw/errorpages/load/	0%	Avira URL Cloud	safe	
http://https://jmcglone.com	0%	Avira URL Cloud	safe	
http://https://tph786.com/sale/images/avatar/	100%	Avira URL Cloud	phishing	
http://kec-rupit.muratarakab.go.id/si/excelz/index.php?email=	100%	Avira URL Cloud	phishing	
http://https://blackberryizm.com/frontend/assets/images/favico/report-fedex.php	100%	Avira URL Cloud	phishing	
http://https://raw.githubusercontent.com/s3cur3th1ssh1t/	0%	Avira URL Cloud	safe	
http://outfish.bounceme.net/outl.dot	100%	Avira URL Cloud	malware	
http://ppaauuaa11232.cc/dlx5rc.dotm	100%	Avira URL Cloud	malware	
http://https://mail.emifermetures.xyz/myguy/receiptswift.php	0%	Avira URL Cloud	safe	
http://103.133.106.72/ini/.....wbk	0%	Avira URL Cloud	safe	
http://www.mygreatlearning.com	0%	Avira URL Cloud	safe	
http://https://myown.bio/vvg	0%	Avira URL Cloud	safe	
http://https://e-secure-log.ga/abu/next.php	0%	Avira URL Cloud	safe	
http://https://greatblueinds.com/ajx-admin/ckeditor/plugins/wsc/dialogs/3o9vbeip3k.php	0%	Avira URL Cloud	safe	
http://https://tpow.zeroworld.xyz/home/application/views/sistem/notifikasi/usqg66westx.php	100%	Avira URL Cloud	phishing	
http://https://browserimprovements.com/check-opt-out?url=$	0%	Avira URL Cloud	safe	
http://windowsdefendergateway.duckdns.org/documents.doc	100%	Avira URL Cloud	malware	
http://83.166.246.59/sgz2/rejoice/lowered.dot	100%	Avira URL Cloud	malware	
http://23.94.174.158/document/invc_00000023444.wbk	0%	Avira URL Cloud	safe	
http://198.23.156.247/receipt/receipt.doc	100%	Avira URL Cloud	malware	
http://192.3.152.171/	100%	Avira URL Cloud	malware	
http://https://url.welimitless.in/bvmms	0%	Avira URL Cloud	safe	
http://https://hide.link/lfspz	100%	Avira URL Cloud	phishing	
http://https://sitesimobisis.com.br/bin/	0%	Avira URL Cloud	safe	
http://103.167.90.69/receipt/inv_126776.wbk	100%	Avira URL Cloud	malware	
http://kitten-268.frge.io/article.html	100%	Avira URL Cloud	malware	
http://https://visualscope.org/visual/office/css/nelz.php	0%	Avira URL Cloud	safe	
http://usb.mine.nu/c.sh-o/users/shared/c.sh	100%	Avira URL Cloud	phishing	
http://trialservice.genesystuna.com/io/excelz/index.php?email=	0%	Avira URL Cloud	safe	
http://49.234.67.167/	100%	Avira URL Cloud	malware	
http://filecopying.xyz/update/kbp08x	100%	Avira URL Cloud	malware	
http://media.vitkvitk.com/xmlstatic/ads/videoplaza/vittalia.html?df=	100%	Avira URL Cloud	malware	
http://3.104.223.22/dhl/receipt.doc	100%	Avira URL Cloud	malware	
http://shdjhgftyhgjklolkjio.dns.navy/bcz/document.doc	100%	Avira URL Cloud	malware	
http://https://pigeonious.com/img/	100%	Avira URL Cloud	malware	
http://swipermachinereview.xyz/wp-includes/t3ow4kf0p0q8oo/	100%	Avira URL Cloud	malware	
http://103.167.93.37/invoice/invoice_000499000049.wbk	100%	Avira URL Cloud	malware	
http://https://rawcdn.githack.net/up.php?key=5	100%	Avira URL Cloud	malware	
http://https://armybar.hopto.org/remoteload.dotm	0%	Avira URL Cloud	safe	
http://private0091111.duckdns.org/qagj/gipsy.png	0%	Avira URL Cloud	safe	
http://https://hosteriaestilonorte.com.ar/admins/uzie/actions.php	100%	Avira URL Cloud	phishing	
http://83.166.246.59/ua-lt98brkc2/perform/luck/	100%	Avira URL Cloud	malware	
http://https://www.mygreatlearning.com	0%	Avira URL Cloud	safe	
http://yourcontents.xyz/0758/0806pn	100%	Avira URL Cloud	phishing	
http://pretence77.glorious.nonima.ru/elenapc/principles/nearly.mp3	100%	Avira URL Cloud	malware	
http://thrprivatecloudshareandfileprotectagent.duckdns.org/receipt/invoice_651254.doc	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://teachon.aerialview.lk/systemdemo/uploads/addons/__macosx/live-class/f2u4p7u3jk.php	100%	Avira URL Cloud	malware	
http://https://fpvtunes.binaryprotectors.com/msreal/jreside	0%	Avira URL Cloud	safe	
http://false.grafitto.ru/dch00-01/rehearsal.dot	100%	Avira URL Cloud	malware	
http://ap.4iitk0-ninv.xyz/?e=u2fuzgkuvghvbxbzb25ay290lnrulmdvdg==	0%	Avira URL Cloud	safe	
http://www.poltc.cz/zackova/novak.exe-outfilec:	0%	Avira URL Cloud	safe	
http://https://office.michiganappellateblog.com/soft.dll	100%	Avira URL Cloud	malware	
http://103.167.90.177/shpdocument/invc_0098008.wbk	100%	Avira URL Cloud	malware	
http://https://ziengineeringco.com/project-arab-contracting/css/dahbzo4xg.php	0%	Avira URL Cloud	safe	
http://https://logz.live/frnd/	0%	Avira URL Cloud	safe	
http://https://wwdurl.com/3nav	0%	Avira URL Cloud	safe	
http://https://bb.realestateprivateportfolio.com/img/	100%	Avira URL Cloud	malware	
http://https://tiger.hotshot.sk/wp-admin/	0%	Avira URL Cloud	safe	
http://https://lidamtour.com/masivo/ala/cronsrt/corn.dot	0%	Avira URL Cloud	safe	
http://earium.ru/ua-lt5cg63120d6/country/	0%	Avira URL Cloud	safe	
http://www.theabigailbloomcakecompany.co.uk/wp-content/uploads/	0%	Avira URL Cloud	safe	
http://https://emicrosoftteam.com/scot/	0%	Avira URL Cloud	safe	
http://www.comeinbaby.com/updateerror/fiif	100%	Avira URL Cloud	malware	
http://209.127.20.13/b44u8j.dotm	100%	Avira URL Cloud	malware	
http://files.telefacer.com/1/2.html	0%	Avira URL Cloud	safe	
http://lump.semara.ru/dch00-01/counter/nearest/	100%	Avira URL Cloud	malware	
http://https://jeffmhall.net/lant/	0%	Avira URL Cloud	safe	
http://https://unlibroparatodos.mx/wp-content/themes/divi/epanel/css/tpcsfltfzf9r7yx.php	0%	Avira URL Cloud	safe	
http://https://www.vespang.cf/sizx/post.php	0%	Avira URL Cloud	safe	
http://atozlovebook.com/vision.iosapp-o%appdata%	0%	Avira URL Cloud	safe	
http://https://extraosseous.com/zik/document.php	0%	Avira URL Cloud	safe	
http://https://lidamtour.com/masivo/ala/cronsrt/	0%	Avira URL Cloud	safe	
http://https://luxtonace.com/luxton/plugins/ckeditor/plugins/a11yhelp/9gysz7pxb.php	0%	Avira URL Cloud	safe	
http://172.245.119.43/recept/34.doc	100%	Avira URL Cloud	malware	
http://107.173.143.102/hhh/invc_005400005400.wbk	0%	Avira URL Cloud	safe	
http://thomastongrealestate.com/skywkc/3415201.pnga	100%	Avira URL Cloud	malware	
http://https://ab.v-mail.online/?e=	100%	Avira URL Cloud	phishing	
http://https://lidamtour.com/masivo/file/kmshost/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.bonusesfound.ml/update/index.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://spr-updates.ddns.net/spr_updates.php-o	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://gengengma.com/wp-content/uploads/vipe_11/send.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp, App16678959291120112000_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://endodermic-needles.000webhostapp.com/clean.php	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false		high
http://https://doocument.m2diving.ml/fay/login.php?log	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://hitechceramics.com/egab/processor.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://shgshgwsdynationalobjindustrialat18ygs.duckdns.org/receipt/invoice_202121.doc	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.sputnikradio.net/radio/news/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	true	• Avira URL Cloud: malware	unknown
http://https://partoniroo.com/n9/u.js&&pingo0.org&&cd	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://acaciavictorias.com/sxmal.php	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://usa-national.info/gpu/band/grumble.dot	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	true	• Avira URL Cloud: malware	unknown
http://https://diarnondfireplace.com/dobo/xxx.php?user=	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://jovial-pasteur.159-89-118-202.plesk.page/wp-content/uploads/index.php	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://tulsabailbondfinancing.com/dglmzmfueublehbmzi5jb20=	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://outfish.bounceme.net/outl.dot	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp, App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://snapper.genesysindonesia.com/excel/excelz/index.php?email=	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://jmcglone.com	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://192.210.240.8/doc_document/188.doc	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://gez.org.zw/errorpages/load/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://www.systweak.com/registrycleaner	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false		high
http://https://tph786.com/sale/images/avatar/	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://kec-rupit.muratarakab.go.id/si/excelz/index.php?email=	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://blackberryizm.com/frontend/assets/images/favico/report-fedex.php	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://raw.githubusercontent.com/s3cur3th1ssh1t/	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp, App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://ppaauuaa11232.cc/dlx5rc.dotm	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://mail.emifermetures.xyz/myguy/receiptswift.php	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mygreatlearning.com	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://103.133.106.72/ini/.....wbk	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://myown.bio/vvg	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://e-secure-log.ga/abu/next.php	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://browserimprovements.com/check-opt-out?url=$	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://greatblueinds.com/ajx-admin/ckeditor/plugins/wsc/dialogs/3o9vbeip3k.php	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://windowsdefendergateway.duckdns.org/documents.doc	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://tpow.zeroworld.xyz/home/application/views/system/notifikasi/usqg66westx.php	notepad.exe, 00000000.00000002.575195265 .000001CF7878C000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://83.166.246.59/sgz2/rejoice/lowered.dot	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://198.23.156.247/receipt/receipt.doc	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://url.welimitless.in/bvmms	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.94.174.158/document/invc_00000023444.wbk	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://hide.link/lfspz	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: phishing	unknown
http://https://transfer.sh/get/0oulld/i9ch18.dotm	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://192.3.152.171/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://sitesimobisis.com.br/bin/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://103.167.90.69/receipt/inv_126776.wbk	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://kitten-268.frge.io/article.html	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://usb.mine.nu/c.sh-o/users/shared/c.sh	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://49.234.67.167/	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://filecopying.xyz/update/kbp08x	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://media.vitkvitk.com/xmlstatic/ads/videoplaza/vittalia.html?df=	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://trialservice.genesystuna.com/io/excelz/index.php?email=	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://visualscope.org/visual/office/css/nelz.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://shdjhgftyhgjklolkjio.dns.navy/bcz/document.doc	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://3.104.223.22/dhl/receipt.doc	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://armybar.hopto.org/remoteload.dotm	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pigeonious.com/img/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://103.167.93.37/invoice/invoice_000499000049.wbk	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://hosteriaestilonorte.com.ar/admins/uzie/actions.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://pretence77.glorious.nonima.ru/elenapc/principles/nearly.mp3	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://private0091111.duckdns.org/qagj/gipsy.png	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://towardsdatascience.com	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://swipermachinereview.xyz/wp-includes/t3ow4kf0p0q8oo/	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://https://rawcdn.githack.net/up.php?key=5	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.mygreatlearning.com	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://83.166.246.59/ua-lt98brkc2/perform/luck/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://bitbucket.org/atlasover/atlassiancore/downloads/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://thrprivatecloudshareandfileprotectagent.duckdns.org/receipt/invoice_651254.doc	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://yourcontents.xyz/0758/0806pn	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://teachon.aerialview.lk/systemdemo/uploads/addons/__macosx/live-class/f2u4p7u3jk.php	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://false.grafitto.ru/dch00-01/rehearsal.dot	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://https://fpvtunes.binaryprotectors.com/msreal/jreside	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ap.4iitk0-ninv.xyz/?e=u2fuzgkuvghvbxbzb25ay290lnrulmdvdg==	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://office.michiganappellateblog.com/soft.dll	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://https://logz.live/frnd/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://103.167.90.177/shpdocument/invc_0098008.wbk	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ziengineeringco.com/project-arab-contracting/css/dahbzo4xg.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.poltc.cz/zackova/novak.exe-outfilec:	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://wwdurl.com/3nav	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://lidamtour.com/masivo/ala/cronsrt/corn.dot	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bb.realestateprivateportfolio.com/img/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://tiger.hotshot.sk/wp-admin/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://earium.ru/ua-lt5cg63120d6/country/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://emicrosoftteam.com/scot/	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://www.comeinbaby.com/updateerror/fiif	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://209.127.20.13/b44u8j.dotm	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://www.theabigailbloomcakecompany.co.uk/wp-content/uploads/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.22find.com/?utm_source=b&utm_medium=	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false		high
http://files.telefacer.com/1/2.html	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://lump.semara.ru/dch00-01/counter/nearest/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://jeffmhall.net/lant/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://unlibroparatodos.mx/wp-content/themes/divi/epanel/css/tpcsfltfzf9r7yx.php	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://atozlovebook.com/vision.iosapp-o%appdata%	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ramashardware.co.za/wp-fxm.php	App16678959291120112 00_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.vespang.cf/sizx/post.php	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://extraosseous.com/zik/document.php	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://172.245.119.43/recept/34.doc	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://luxtonace.com/luxton/plugins/ckeditor/plugins/a11yhelp/9gysz7pxb.php	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://https://lidamtour.com/masivo/ala/cronsrt/	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: safe	unknown
http://thomastongrealestate.com/skywkc/3415201.pnga	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: malware	unknown
http://https://lidamtour.com/masivo/file/kmshost/	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ab.v-mail.online/?e=	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log	false	• Avira URL Cloud: phishing	unknown
http://107.173.143.102/hhh/invc_005400005400.wbk	notepad.exe, 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	743454
Start date and time:	2022-11-10 21:14:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log
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:	4
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.expl.evad.mine.winLOG@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .log

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com

- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

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:	data
Entropy (8bit):	7.001609475452913
TrID:	• MP3 audio (ID3 v1.x tag) (2501/1) 71.42% • MP3 audio (1001/1) 28.58%
File name:	App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log
File size:	20971520
MD5:	988e0cb19fbc2cf5e3b9a33b205affd8
SHA1:	1b091e30aa366a5cdf582a81954893ac6201f769
SHA256:	c289adee6ca95bb69f864497f32a8abbad65d20dccd06c4a1f6c3ef6d402693d
SHA512:	03b01dce8b2e53d4aa3735483cc0111298f02e31fc21010da57a0c31b8d8340170d3d74639e658f7f45456c11d811b025e26f4131d646112038d3f79c844f84c
SSDEEP:	196608:4qvvbS9+lFh9AUwoupfvAdcUPPEXoElJfEt3nvpn0A9bkWAJLaJEtTiVJkQ5uZTz:4K3lFh9Q7NXltEFvpn07YUiUF//dhr5
TLSH:	8427AE5BB3A400E4D1B6C274C5169B67EBB27C0A1B2197CB1760765A2F336F18A3B3D1
File Content Preview:	.K...jjccbbflaster1.ocxflaster3.ocxpasel32kernwnloadtoflaster2.ocxc:\nasterosa..)...-!#SCPT:TrojanDownloader:O97M/Qakbot.PDO85!MTB.....K...c:\hefaggad\ukdfaovkga\buuefafa.dll...c:\hefaggad\ukdfaovkga\buuefafb.dll..)...-!#SCPT:TrojanDownloader:Win32/Lnkge

File Icon

Icon Hash:	74f4e4e4e4e4e4e4

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: notepad.exe PID: 5416, Parent PID: 3324

General

Target ID:	0
Start time:	21:15:40
Start date:	10/11/2022
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\Desktop\App1667895929112011200_34122CF1-AE58-41FB-8E13-C906CB8D40E6.log
Imagebase:	0x7ff6b07c0000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source: 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_PWSH_PasswordCredential_RetrievePassword, Description: Detects PowerShell content designed to retrieve passwords from host, Source: 00000000.00000002.575195265.000001CF7878C000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly