ID: 450276
Sample Name: ms.bin
Cookbook: default.jbs
Time: 22:36:15
Date: 17/07/2021
Version: 33.0.0 White Diamond

Table of Contents

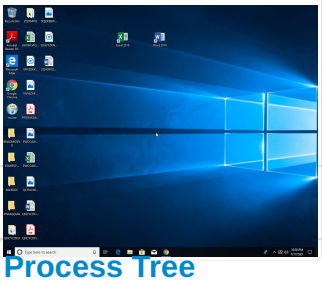
Windows Analysis Report ms.bin

Overview

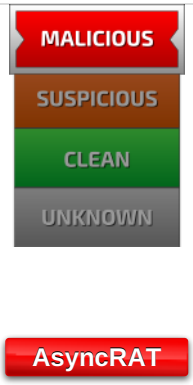
General Information

Sample Name:	ms.bin (renamed file extension from bin to exe)
Analysis ID:	450276
MD5:	dbbb611daf3abd4.
SHA1:	1b33772f2acc9e6..
SHA256:	d5a8b6cb7b39d6..
Tags:	Async exe
Infos:	

Most interesting Screenshot:



Detection

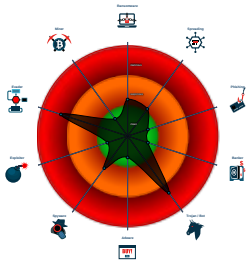


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Yara detected AsyncRAT
- .NET source code contains potentia…
- Connects to a pastebin service (like…
- Contains functionality to check if a d…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Sigma detected: Regsvr32 Anomaly
- Tries to detect sandboxes and other…
- Uses schtasks.exe or at.exe to add …

Classification



Process Tree

- **System is w10x64**
- ms.exe (PID: 4156 cmdline: 'C:\Users\user\Desktop\ms.exe' MD5: DBBB611DAF3ABD47972AE4FAF5D54C95)
  - ASTRO-GREP.EXE (PID: 5416 cmdline: 'C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE' MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
    - cmd.exe (PID: 912 cmdline: 'C:\Windows\System32\cmd.exe' /c schtasks /create /f /sc onlogon /rl highest /tn 'astro-grep' /tr "C:\Users\user\AppData\Roaming\astro-grep.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5996 cmdline: schtasks /create /f /sc onlogon /rl highest /tn 'astro-grep' /tr "C:\Users\user\AppData\Roaming\astro-grep.exe" MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 3352 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\tmp7B21.tmp.bat" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 1364 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - astro-grep.exe (PID: 2792 cmdline: 'C:\Users\user\AppData\Roaming\astro-grep.exe' MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
  - ASTROGREP_SETUP_V4.4.7.EXE (PID: 3728 cmdline: 'C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE' MD5: A708211241313FEAF9621E571631534D)
- astro-grep.exe (PID: 748 cmdline: C:\Users\user\AppData\Roaming\astro-grep.exe MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ms.exe	Malware_QA_update	VT Research QA uploaded malware - file update.exe	Florian Roth	• 0xa0a8:$x4: C:\Users\DarkCoderSc\ • 0xa0c5:$x5: Celesty Binder\Stub\STATIC\Stub.pdb
ms.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
C:\Users\user\AppData\Roaming\astro-grep.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.250713765.0000000002A4E000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000D.00000000.253043295.000000000772000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000003.00000000.197769647.00000000005F2000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000003.00000002.250001680.00000000005F2000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000001.00000002.200014509.0000000000A3F000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.astro-grep.exe.430000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.0.ASTRO-GREP.EXE.5f0000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
1.2.ms.exe.a3f330.2.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
13.2.astro-grep.exe.770000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.ASTRO-GREP.EXE.5f0000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 11 entries				

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Anomaly

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Connects to a pastebin service (likely for C&C)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AsyncRAT

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

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Lowering of HIPS / PFW / Operating System Security Settings:

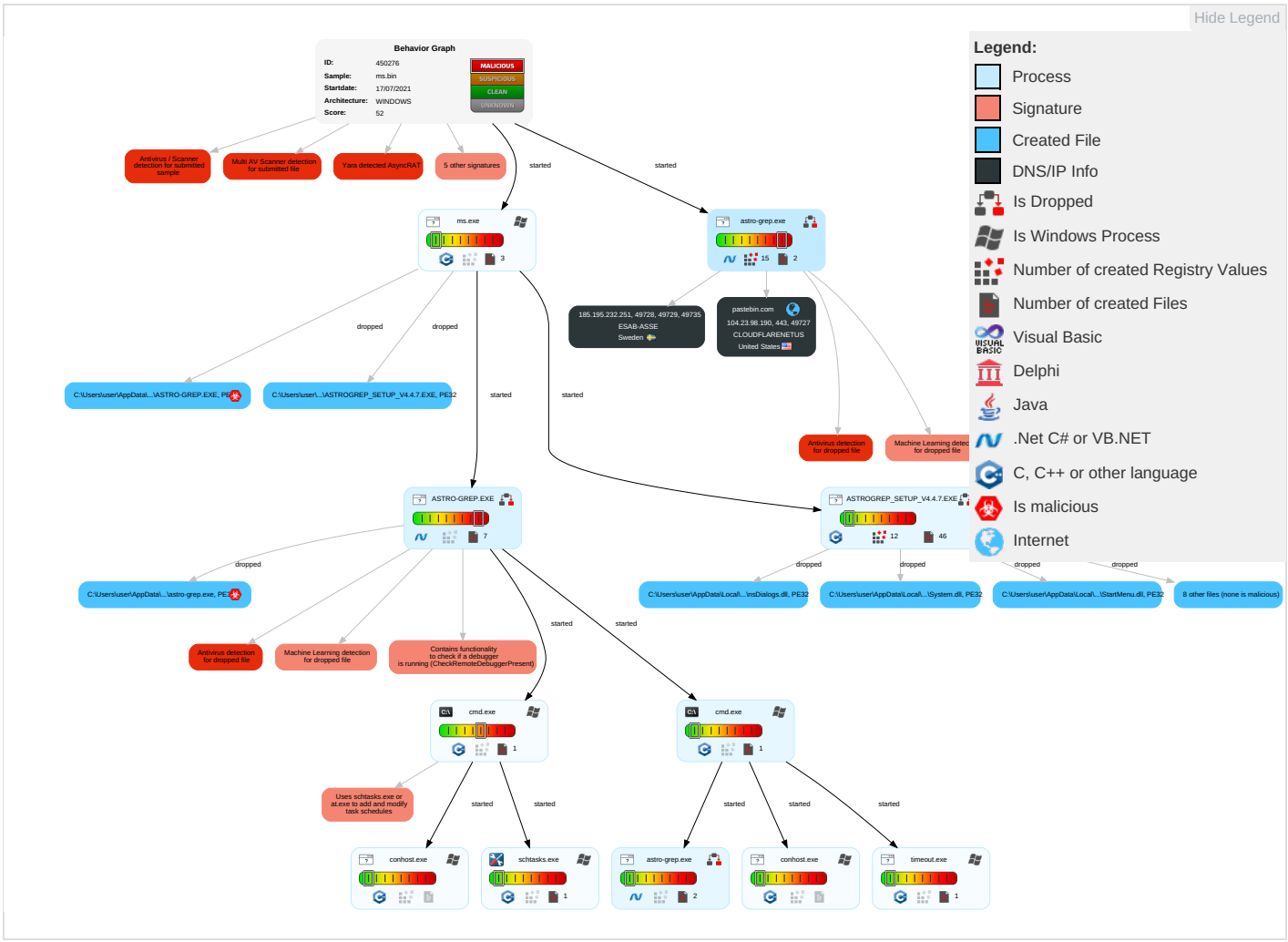
Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 2	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eavesd Insecur Networ Commu
Default Accounts	Scripting 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Scripting 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit Redirec Calls/S
Domain Accounts	Native API 1	Logon Script (Windows)	Scheduled Task/Job 2	Obfuscated Files or Information 1 1 1	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploit Track D Locatio
Local Accounts	Command and Scripting Interpreter 2	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Scheduled Task/Job 2	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

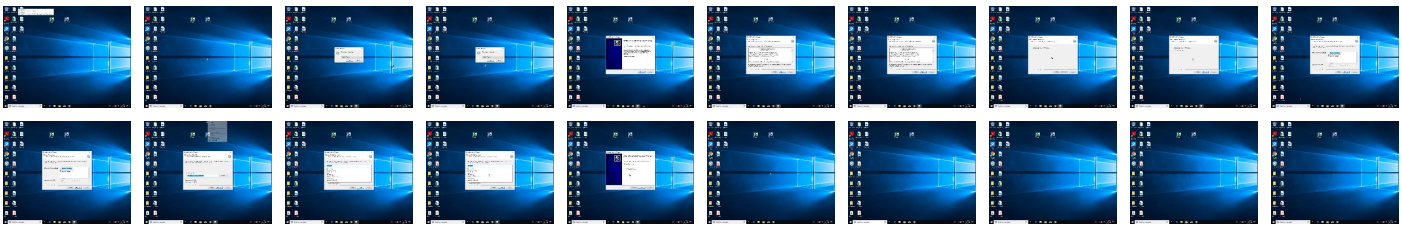
Behavior Graph



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
ms.exe	78%	Virustotal		Browse
ms.exe	100%	Avira	TR/Dropper.Gen	
ms.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\astro-grep.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\astro-grep.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe	0%	Virustotal		Browse
C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe	0%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe	0%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\AstroGrep.Common.dll	0%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\AstroGrep.Common.dll	0%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\AstroGrep.exe	2%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\AstroGrep.exe	0%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\ICSharpCode.AvalonEdit.dll	0%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\ICSharpCode.AvalonEdit.dll	0%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\NLog.dll	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\AstroGrep\NLog.dll	0%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\Uninstall.exe	5%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\Uninstall.exe	2%	ReversingLabs		
C:\Program Files (x86)\AstroGrep\libAstroGrep.dll	0%	Metadefender		Browse
C:\Program Files (x86)\AstroGrep\libAstroGrep.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE	4%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.ASTRO-GREP.EXE.5f0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.ASTRO-GREP.EXE.5f0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.astro-grep.exe.430000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.astro-grep.exe.770000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.0.ms.exe.a30000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.astro-grep.exe.430000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.0.ms.exe.a4b130.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.astro-grep.exe.770000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.ASTRO-GREP.EXE.2a4e31c.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
1.2.ms.exe.a4b130.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.ms.exe.a30000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://pastebin.com43l	0%	Avira URL Cloud	safe	
http://https://pastebin.comD83l	0%	Avira URL Cloud	safe	
http://https://pastebin.comD83lh;	0%	Avira URL Cloud	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://schemas.microsof	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pastebin.com	104.23.98.190	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.195.232.251	unknown	Sweden		39351	ESAB-ASSE	false
104.23.98.190	pastebin.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450276
Start date:	17.07.2021
Start time:	22:36:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ms.bin (renamed file extension from bin 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:	34
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:	mal52.troj.evad.winEXE@19/26@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.8% (good quality ratio 11.6%) • Quality average: 70% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:37:25	Task Scheduler	Run new task: astro-grep path: "C:\Users\user\AppData\Roaming\astro-grep.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.195.232.251	astro-grep-setup.exe.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	
104.23.98.190	C1jT7pIYSJ.exe	Get hash	malicious	Browse	• pastebin.com/raw/npsqXhuQ
	uwoYazbVds.exe	Get hash	malicious	Browse	• pastebin.com/raw/npsqXhuQ
	u6Wf8vCDUv.exe	Get hash	malicious	Browse	• pastebin.com/raw/BCAJ8TgJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EU441789083.doc	Get hash	malicious	Browse	• pastebin.com/raw/BCAJ8TgJ
	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	E1Q0TjeN32.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6YCl3ATKJw.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	Hjnb15Nuc3.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	4av8Sn32by.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	5T4Ykc0VSK.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	afvhKak0Ir.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	T6OcyQsUsY.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KITgJnGbl.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PbTwrajNMX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	22NO7gVJ7r.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	rE7DwszvrX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VjPHSJkwr6.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	astro-grep-setup.exe.doc	Get hash	malicious	Browse	• 104.23.98.190
	TIJYYlYJpv.exe	Get hash	malicious	Browse	• 104.23.99.190
	banload.msi	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.PackedNET.721.17987.exe	Get hash	malicious	Browse	• 104.23.98.190
	6rg5Enu1ks.exe	Get hash	malicious	Browse	• 104.23.99.190
	Loader.exe	Get hash	malicious	Browse	• 104.23.99.190
	banload.msi	Get hash	malicious	Browse	• 104.23.98.190
	t3uss3bjUL.exe	Get hash	malicious	Browse	• 104.23.98.190
	h3Y0CRAJyq.exe	Get hash	malicious	Browse	• 104.23.98.190
	Order Request.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	4fy0Wb1EUX.exe	Get hash	malicious	Browse	• 104.23.98.190
	CYzY9Pi2ny.exe	Get hash	malicious	Browse	• 104.23.99.190
	SgCDxPdEul.exe	Get hash	malicious	Browse	• 104.23.99.190
	42C75D53ACD263FF2B2DAD511E40E0E40E9A6119BAA68.exe	Get hash	malicious	Browse	• 104.23.99.190
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	Lr2Hm9rVac.exe	Get hash	malicious	Browse	• 104.23.98.190
	XoN2GgRiga.exe	Get hash	malicious	Browse	• 104.23.99.190
	vEJ2Mfxn6p.exe	Get hash	malicious	Browse	• 104.23.99.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	G-DECL G50 EURL.xlsx	Get hash	malicious	Browse	• 104.23.99.190
	C1jT7pIYSJ.exe	Get hash	malicious	Browse	• 104.23.98.190

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	astro-grep-setup.exe.doc	Get hash	malicious	Browse	• 104.23.98.190
	glupteba.exe	Get hash	malicious	Browse	• 104.21.63.250
	E2QlvDXi7H.exe	Get hash	malicious	Browse	• 104.21.83.89
	JHECEQl1ML.exe	Get hash	malicious	Browse	• 172.67.220.44
	UwvHsxxlTi.exe	Get hash	malicious	Browse	• 104.21.19.209
	gVI2lrBzjJ.exe	Get hash	malicious	Browse	• 172.67.201.250
	y54fD0dMcF.exe	Get hash	malicious	Browse	• 104.21.87.184
	WR0MTpWkYC.exe	Get hash	malicious	Browse	• 172.67.193.180
	LPY15536W4.exe	Get hash	malicious	Browse	• 104.21.84.71
	SecuriteInfo.com.Trojan.Inject4.14369.15008.exe	Get hash	malicious	Browse	• 162.159.134.233
	TIJYYlYJpv.exe	Get hash	malicious	Browse	• 162.159.138.232
	7vLHRD4IdanbLrE.exe	Get hash	malicious	Browse	• 104.21.19.200
	PTELOONB39-67.exe	Get hash	malicious	Browse	• 172.67.215.158
	o2fAkrQ43w.exe	Get hash	malicious	Browse	• 104.21.51.99
	ATT62725.HTM	Get hash	malicious	Browse	• 104.18.11.207
	WAdStf9Llw.exe	Get hash	malicious	Browse	• 104.21.51.99
	P.O 16.exe	Get hash	malicious	Browse	• 104.21.19.200
	F6w8Ll8iWU.exe	Get hash	malicious	Browse	• 162.159.133.233
	PCgYjH5fEn.exe	Get hash	malicious	Browse	• 104.21.19.209
	another.dll	Get hash	malicious	Browse	• 104.20.185.68
ESAB-ASSE	astro-grep-setup.exe.doc	Get hash	malicious	Browse	• 185.195.232.251
	TIJYYlYJpv.exe	Get hash	malicious	Browse	• 185.65.135.248
	NotificationApplicationspdf.exe	Get hash	malicious	Browse	• 141.98.255.146
	SgCDxPdEul.exe	Get hash	malicious	Browse	• 185.65.135.248
	5icstaf5i1.exe	Get hash	malicious	Browse	• 45.83.220.209
	aY5UWK4jxg.exe	Get hash	malicious	Browse	• 45.83.220.209
	ewlD3Dwdxy.exe	Get hash	malicious	Browse	• 185.65.134.182
	byodInstCL.exe	Get hash	malicious	Browse	• 193.32.127.38
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 185.195.232.251
	PD0ssyK178.exe	Get hash	malicious	Browse	• 185.65.134.173
	EpVgl7WUGD.exe	Get hash	malicious	Browse	• 185.65.134.173
	tgv7RXFab7.exe	Get hash	malicious	Browse	• 185.65.134.173
	7niXcdi1SU.exe	Get hash	malicious	Browse	• 185.65.134.173
	9gee3iCc4N.exe	Get hash	malicious	Browse	• 185.65.134.173
	l3eFnAYO6a.exe	Get hash	malicious	Browse	• 185.65.134.173
	X97zFKQz4Q.exe	Get hash	malicious	Browse	• 185.65.134.173
	jf1w8rsogr.exe	Get hash	malicious	Browse	• 185.65.134.173
	s1G5ZwG3Yb.exe	Get hash	malicious	Browse	• 185.65.134.173
	3ZhSP5SXgW.exe	Get hash	malicious	Browse	• 185.65.134.173
	wvS1iVG3MK.exe	Get hash	malicious	Browse	• 185.65.134.173

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	y54fD0dMcF.exe	Get hash	malicious	Browse	• 104.23.98.190
	SO-19844 EIDCO.ppam	Get hash	malicious	Browse	• 104.23.98.190
	TIJYYlYJpv.exe	Get hash	malicious	Browse	• 104.23.98.190
	7vLHRD4IdanbLrE.exe	Get hash	malicious	Browse	• 104.23.98.190
	IdDetails.ppam	Get hash	malicious	Browse	• 104.23.98.190
	P.O 16.exe	Get hash	malicious	Browse	• 104.23.98.190
	F6w8Ll8iWU.exe	Get hash	malicious	Browse	• 104.23.98.190
	Sirus.exe	Get hash	malicious	Browse	• 104.23.98.190
	New Purchase Order-030220.ppt	Get hash	malicious	Browse	• 104.23.98.190
	ReGQ1vAQp9.exe	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_119040 Beleg.ppt	Get hash	malicious	Browse	• 104.23.98.190
	order 0721 Review .doc.exe	Get hash	malicious	Browse	• 104.23.98.190
	6rg5Enu1ks.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ REF R2100131410 pdf.exe	Get hash	malicious	Browse	• 104.23.98.190
	samples.exe	Get hash	malicious	Browse	• 104.23.98.190
	265.exe	Get hash	malicious	Browse	• 104.23.98.190
	Loader.exe	Get hash	malicious	Browse	• 104.23.98.190
	Supwaize2.exe	Get hash	malicious	Browse	• 104.23.98.190
	download.dat.exe	Get hash	malicious	Browse	• 104.23.98.190
	WindowsFormsApp1.exe	Get hash	malicious	Browse	• 104.23.98.190

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\AstroGrep\ICSharpCode.AvalonEdit.dll	astro-grep-setup.exe.doc	Get hash	malicious	Browse	
C:\Program Files (x86)\AstroGrep\AstroGrep.Common.dll	astro-grep-setup.exe.doc	Get hash	malicious	Browse	
C:\Program Files (x86)\AstroGrep\NLog.dll	astro-grep-setup.exe.doc	Get hash	malicious	Browse	
C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe	astro-grep-setup.exe.doc	Get hash	malicious	Browse	
C:\Program Files (x86)\AstroGrep\AstroGrep.exe	astro-grep-setup.exe.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	7168
Entropy (8bit):	4.487949196682819
Encrypted:	false
SSDEEP:	96:+2x9scF3MzO5l+9B9Q6uyT4A3KXr7HazHJ/ylHj/V3ojWNta1FYcCe:5x938OYLsA3YgwN5RszYcCe
MD5:	A06B34EE8AD3B52CE1C76847FC7991A0
SHA1:	D52CBED52AD91E5D297E3F96D7AAA1476A42F087
SHA-256:	0822F460D448356DAE96963C1A56DA2553FE6BB6A859B1646D1A76DBC346F03C
SHA-512:	B4741046E83A89FBFB8848AC649E22D1773B54F5B6C96EE49057C12ADE502DE5594C706BAE140FEF864F3FB1A585A0F8D840C5369073561189C9665CD5FD2CD
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: astro-grep-setup.exe.doc, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....G.\.....-... ...@....@.. ....@.....,..S....@..P.....`.....+..... ..... ..H.....text...4.... ..... ..`.rsrc...P....@.....@..@.rel oc.....`.....@..B.....-.....H.....".....0..T.....i.1M..i.0G..~.....r...p.....(....&...r)..pr-..po.....r)..pr-..po.....(....*.0..... ~....r/..p.o.....~....rO..p.o.....~....r...p.o.....9q....9k....9e....99....r...po.....r...po.....r...po.....93.....9,.....9%....r-..p.r...p(....o.....r-..p.r...p(....o.....r-..p.r...p(....o.....r...pr...p.(....o. .....r...pr...p.(....o.....r...pr...p.(....o.....r...po.....r...po.....r.

C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe.config	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	175
Entropy (8bit):	5.022488547778473
Encrypted:	false
SSDEEP:	3:vFWWMNHU8LdgCQcIMOoT02VK/FlURAmIRMNHjFHr0lUfEyhTRRAoe+RAW4QIMOov:TMVBd1l002VKNa7VJdfEyFRRAoeuAW44
MD5:	57717DA46BD278CA043D8101847D8FF4
SHA1:	D93BAADBB3C644D841D7AA4E95DCD76F9897BD05
SHA-256:	12D08F2857A02B5A4EF5DF6EC2D840296AAC4C219704B2FB6F15A7571230A4C5

C:\Program Files (x86)\AstroGrep\AstroGrep.AdminProcess.exe.config	
SHA-512:	A054A7FD69E4A643286212FEDABDE4BDFB36BBF3E7F9FC33524BA8DFECBC375E991C23B4E047F5F235A77E9D6A525F996934A4A993B61E1FE7D84066FF972DI 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>...<startup>.. <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>...</startup>..</c onfiguration>..

C:\Program Files (x86)\AstroGrep\AstroGrep.Common.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	4.660156886149009
Encrypted:	false
SSDEEP:	192:MPL93AfzEbqrlLH945OKtueaQJ6BLcSEeC137:MsEbyHGscu3DdkxL
MD5:	2F2899673ABB136BFC8B92A6D3BAFF33
SHA1:	5BE14D5C58AF9F78858DD5E9ED6CD929F87AC0B4
SHA-256:	0E7A71232FB6676777A823ADDB4776BD895ABBE29EA2487110073BD0C5FF6AA6
SHA-512:	CF5B23F4E5417DDC4AB5A354E7EA90C5CCE28133DE7D1AE260F0879E474727DBB73E47C9CB92A98BD5B6F6EBCFC67CD955423FA1615A0D7C24783415325200 A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: astro-grep-setup.exe.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.\.....!.....9... ...@..... ....@.....9..K....@.....`.....H8..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....".....@..B.....9.....H.....@$.....(....,(....o....(....*..(....~....(....*...0.....(....r...p(.....(....r...p(.....~....~....r...p(.... (.....~....~....r...p(....(.....(....o....(.....(....o....(.....*..(....*..{....*"..}....*..{....*"..}....*^~....-.s.....~....*..0.....(....s.....s.....r1..p.o.....~....}.....{....(....o.....~....(....o.....r;..p(. ...o .... ..P.jo!.....o".....o#...r...p~$....s%...

C:\Program Files (x86)\AstroGrep\AstroGrep.exe	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	573440
Entropy (8bit):	6.183835631467389
Encrypted:	false
SSDEEP:	12288:uibf6/zxXrXyhwSl9LndCXlhqNWvgVYODH9zG5X1LeihaBQSa:ifEWOYODH9zoX1Le/
MD5:	202C965DE1291E773F7DAE0C495253FB
SHA1:	13EB40E5DF525388D7A2AD18B1720FED78C5EE13
SHA-256:	3138155ABD6A9BADDB63869CD34BF0492718929E910CB4F38BC1767507932B4F
SHA-512:	97445E848DA86876AB324B9C6EC2D27F51BE753ABF1956A79829763F92363B9B7C05A232F876C97A66653109505BAE94BB2B85B53E6F9697698EF8EA2FD21F7A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: astro-grep-setup.exe.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.\.....0.....E... ...`..... ..... ..@.....E..W....`...i..... ....H.....text...&... ...0..... ..`.rsrc....i...`...p...@.....@..@.rel oc.....@..B..... ....

C:\Program Files (x86)\AstroGrep\AstroGrep.exe.config	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	237
Entropy (8bit):	4.960108368394514
Encrypted:	false
SSDEEP:	6:TMV0klffVKNC7VJdfEyFRRAopuAlKNjSt+gP9XWRM5W4QIT:TMG13VOcr6U9wNutJP9UMo4xT
MD5:	502C63E84CACC88FA782EEC1772EFF68
SHA1:	BA6138741633C60D1C92C7C25DDE15D378C0C324
SHA-256:	FE3405C9535DCE3857908E6740099227B7D55CF78A15676D440E781E04EA17BD
SHA-512:	EBA2DD5216BB3293BB3101A5CDADDEF0B4A94577159A8A0654F712F9939F1D03FF670DA6DF0B5F4475D593EDDF330E76E2F6EB19B19E3E51C2EA53A74ACC59 B3

C:\Program Files (x86)\AstroGrep\AstroGrep.exe.config	
Malicious:	false
Preview:	<?xml version="1.0"?>..<configuration>.. <startup>.. <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>.. </startup>.... <runtime>.. <gcAllowVeryLargeObjects enabled="true" />.. </runtime>..</configuration>

C:\Program Files (x86)\AstroGrep\AstroGrep_256x256.png	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6813
Entropy (8bit):	7.898680227457462
Encrypted:	false
SSDEEP:	192:djkp/iNmEYXGtZEV2QWEgFmPPqlqCSKG1Ief:hmiNmTP733q+XR
MD5:	2143826EABE773D3206333B65C2FC67B
SHA1:	B75806940C971C2BB8584E1028EFA512F8AA5646
SHA-256:	8A50671F22D64A0131C9FFE23B3777862172F6D5C63B48C94DFE0FE8E8D62D06
SHA-512:	3D0611BEE13D6A397D5FB3F2E924829360596891DBCFDE1EC0FCE25F2DDEE62D50A10ABA31827334FE12867C508694BB8FB3F72604FC08A1CD323C2615C2F3F
Malicious:	false
Preview:	.PNG.....IHDR.....\r.f....sRGB.....gAMA.....a.....pHYs...3...3.\.....tEXtSoftware.paint.net 4.0.5e.2e....IDATx^.=.]Uv.).....Gr1.....<....K...((((\X.....<.'r...f... I..D@.`.3a&.B.C...``.0~o.....y...{...?.K.....Z.....u..mS8.~.W..c..i.4x..M\J\....v..S...s.=....1....!U.S.Ri...w...N.3....>.....2..,...2.T6...J3.).../.....*.....{.....xN....`.i.m._.j.E*.fap.'.K`. /.Mp...xc...,.z...F...Ri.....<.x.....qOW2..6..L.....UWfX...8....t...[..t...*{Y7.....4.E*....9hw...|.t..s.R.....=..."`.....T...v.o..W=.y.|.....4Y.....H.Y.8&.....|w...~.X...X....-.bH...8...^.]...~. ....y....'%-.T.....^.2..k.9.%.&Y....w..D*.4p....>_=.7>l.n2.<..1...4w.3%.....G....M...epL....T.I.s4....x.n.i.f=...V.?.6.....e.,.$.....).n.q..Q..-#.-....W:I8L.W.M.-...+.h..l.8...si.r.S...N..... ...!.b.....hk.N|..P>..RY;h...7.....9wBzH.J.He...../.F'..7]..o.|.V..F.....1A..}.....@c.....%^.gf.....~..T.....|1...:f^.W.;O*...,.4.....E...}...k.#.%

C:\Program Files (x86)\AstroGrep\ICSharpCode.AvalonEdit.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	626688
Entropy (8bit):	6.014937851800105
Encrypted:	false
SSDEEP:	6144:Oo7n6u1n5vp9yRUmqtM0yRrl0pjoeUy8b01vKbZ/gAGl0gUEdYC:OoLDnwmW0yRr88bwKKdf
MD5:	B4D5D46E50006E87B30E7D514E95173C
SHA1:	BD3BA298EB7E4CDBFDF29E3992BE7D32A4E792EB
SHA-256:	058F38F33F3F99F904AB9588447A234346C859718404B4E8A523673ED19CDBE7
SHA-512:	38FF7CADA6CFA56AF812A1D859AAC4FB8B94DF50454A9FECC55E4FDB159339F6BA885D0B57FE8C522227DD9280CDA0CA21C6A073B6552923FA33F6E77D8F3E C5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: astro-grep-setup.exe.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....f.Y.....!.....`... .....~.... .....@.. .....)... ..@.....,...O.....8.....}..... ..... ..H.....text...._... ...`..... ..`.rsrc...8.....p.....@..@.rel oc.....@..B..... ....

C:\Program Files (x86)\AstroGrep\NLog.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	784384
Entropy (8bit):	6.017097344038701
Encrypted:	false
SSDEEP:	12288:/n77J/zrlPjThZdvTU585ZqmjlJzAF7GVj8TcpkMcaQD3SaB5mUsQ:/n77J/zrlPjThZdv55ZbIF7GVje4kRD5
MD5:	063D7646038B3676CA4BBCCF8CD9736C
SHA1:	DE90082E366938A3D1BB16A9B5BBB4D692F620D4
SHA-256:	F809128B8E35F20A0407F9642AEFA1A64D2B5494F024F5EC403B712C67441ECD
SHA-512:	BB50F12A9B5DE65752B7AFDDF82726A82BB06DF8B6B16712385663981DA810189FA9B72FA45122B3C57719D9EB626BB5D1D90B29D833851A4AA08E35B6FDB92
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: astro-grep-setup.exe.doc, Detection: malicious, Browse

C:\Program Files (x86)\AstroGrep\NLog.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#....." ..0..... .. ..`.....0... ..@.....3...O.... .....@.....d...T..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....g.....H.....L.....4.....".(...*..(...*"..(...*..(...*..(...*..(...*"..(...*...0..B.....~.....(X...~....,.~.... .oY.....+...(.....oZ.....,..([....*...../7....."..(...*6.(.....(S...*..0.....(.....o\...&.*.(....o]...*2(.....oY...*....0..?.....~.....(X...~....,.~.....oY...+...(.....o^...&...,..([....*.....,4.....0 ..?.....~.....(X...~....,.~....o_.....+...(....o`.....,..([..

C:\Program Files (x86)\AstroGrep\Uninstall.exe	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	61854
Entropy (8bit):	6.589895956298641
Encrypted:	false
SSDEEP:	1536:Gw4fpS/nScizHM74N0DIDidcfgdLeAyN9jWtNixGl:Gw4gnScG4DI2dcfceAkWrixq
MD5:	15BDDE25A8A23AAFB0E593D4A1F145B6
SHA1:	250EC8FEA74A2EAC9A1BD3DA1ABF5AC91D1962D7
SHA-256:	4118177FBD02533C449D3D02168300DA1D5B24052B10877A3B4BC03E27C5C375
SHA-512:	3AFB05064722B5616EA74BC8C8E6C50D6EB8F1125AC333339430D05FAE89E445753E45DD5FDCA17E9BE9A94BCA67B3E2B31EEB52DAF2AF3BEC47D0A1EC1AB D03
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...F...F...F.*.....F...G.v.F.*.....F..v...F...@...F.Rich..F..... .....PE..L....z.W.....`...|.....1.....p....@.....@.....4u.....pP.....p..... ....text...._.....`..... ..`.rdata..R....p.....d.....@..@.data....T.....x.....@....ndata.....rsrc...pP.....R...~.....@..@..... ....

C:\Program Files (x86)\AstroGrep\astrogrep.VisualElementsManifest.xml	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	303
Entropy (8bit):	5.268121017723893
Encrypted:	false
SSDEEP:	6:ejHyWc4subuVFWod/NDhkQwYnF4kQwYWadTZ/FhYWadTZ/FeXXKhdNc0SDSFQ:ebvyWW/meZsR1sR8drDGQ
MD5:	824E6132D30D647AED6E9EE3C2DA12C9
SHA1:	DCBE8CAB6784AA26BC9A4F0DC5B60D9733A49F74
SHA-256:	01BF1A694FAF44953B592D1C237D3F93C1B8B346476C30E638C1FAAD0201386B
SHA-512:	DABC61D48723B53C95EE7BBDDB92261E724054CDCE4F9616B0338CACE8F8A9667CAC087C131D8A83BEE68875436F08F9A313F70EA5B85A46989D2B21C84F05 1
Malicious:	false
Preview:	<Application xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>.. <VisualElements.. ShowNameOnSquare150x150Logo='on'.. Square150x150Log o='AstroGrep_256x256.png'.. Square70x70Logo='AstroGrep_256x256.png'.. ForegroundText='light'.. BackgroundColor='#fb7f06'/>..</Application>

C:\Program Files (x86)\AstroGrep\libAstroGrep.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	237568
Entropy (8bit):	5.286872988422086
Encrypted:	false
SSDEEP:	3072:1QwCS0adLYzS+L5VsbeNcg2lZOz3eJJ9oA3fGu51O+q4gbPaYgVXLRn/qR8H6K69:1QwCAdLy/mucxIUKPOufGu5m4fr
MD5:	6E3AFEF0BD6B7EC03007CCDD76F85447
SHA1:	8B434EAB09D948FAC57E98F312C8B24381873374
SHA-256:	B268CDA0D5F431E0CB86FFF8A39420AC03DFC9C498CAE702F859904B79307EDE
SHA-512:	E10EC66C764584AD80D47C1B0CF64B61EBBE3B4E72D2CA05BCDAB5B62F4E3F6FE17A1C37EED9D87A678B8C3D42E6534DE9EE95BF204CA815426EA28935633 94
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.\.....!.....n.... ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....X.....^~....-.s.....~...*...}..... .I..}.....(.....{....s....}.....s....}....*6.{.....o....*v.{.....o.....{.....o....*.*r. {.....o.....{.....o....&*..0.....{.....o....(.{.....o....{.....o....&.{.....o....&*.{.....o.....{....o.....{....1'.{....{....o....o ...o!...&.{....o"....{.....o....&*..0.....(.....(#...o$...r...p.{....o.....o...+.s&. ....o'...o(...-..o'...o).....s*.....s+....s,....

C:\Program Files (x86)\AstroGrep\license.txt	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18330
Entropy (8bit):	4.736471809051081
Encrypted:	false
SSDEEP:	384:lq2PmwEPb6k1iAVX/dUY2ZrEGMOZt7o0sDTj:lzuVLiY+rTZo0sDTj
MD5:	1324A1677693CF2A399CC9424C756CC3
SHA1:	2F29E68AB545965C401A12CE4783F7314E658AF3
SHA-256:	A4BD518E7F66B63A62035C0C542B5F3287BAF7138E13A0F6A30781D8730D766A
SHA-512:	2FD47275325B3605A9B982704BABFAD72D5AF3048064C66554F00F4D4D264DF252697F1D52733F6C87FBB3927A9FDD48ACF94B2E9475FD52334EFA12EA9F0B5A
Malicious:	false
Preview:	.. GNU GENERAL PUBLIC LICENSE.... Version 2, June 1991.... Copyright (C) 1989, 1991 Free Software Foundation, Inc... 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.. Everyone is permitted to copy and distribute verbatim copies.. of this license document, but changing it is not allowed..... Preamble.... The lic enses for most software are designed to take away your..freedom to share and change it. By contrast, the GNU General Public..License is intended to guarantee your freedom to share and change free..software--to make sure the software is free for all its users. This..General Public License applies to most of the Free Software..F oundation's software and to any other program whose authors commit to..using it. (Some other Free Software Foundation software is covered by..the GNU Library G eneral Public License instead.) You can apply it to..your programs, too..... When we speak of free software, we are referring to freedom, not..price. Our General Publi

C:\Program Files (x86)\AstroGrep\readme.txt	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1834
Entropy (8bit):	4.931632926415765
Encrypted:	false
SSDEEP:	24:CGEEY1zF17X+B41FcMEEn+0MJ/cIr3EQZ1WrT5M5tmZNijpibbCT32yvosGQC:tYFFN+B41eM2UvQL0T1Fzy/GZ
MD5:	ABE9A78B3FD8ECD7409C2B382820134E
SHA1:	9AEC458EA30060EE633BD25D235C02AAEFF989D1
SHA-256:	B17BBDB71C888116A8661B373CA088C9B174E00551DF81B887EE9BCA28492189
SHA-512:	0F554B3BA4749B22728D303B7AC1BD7596CCAE5A51D0F06560AA829222DD5DFF31F089C2D5894A23D97093836A76595EA5BAA4441EAC4DF44C321F14CD554A3
Malicious:	false
Preview:	.Changelog for AstroGrep v4.4.7..==========..Bugs..-85: Possible issue with word plugin and leaving winword.exe process open...-98: Error "the string was not recognized as a valid DateTime"..-100: Performance issues..-101: Searching Multiple MS Word Doc uments..-102: Context Lines Display Discrepancy..-103: Astrogrep 4.4.6 hangs clicking on found file..-104: commandline spath not accepting multiple searchPath..-108: Used ListSeparator on right mouse "Copy all"..-109: Command Line issues - Check logic and docs..-113: Feature 108 is not working (Add additional text editor parameter for search text)....Featured Requests:..-101: Stopped painting status bar as often..-110: Exclude directories that do not match pattern (added not equals option for path based options)..-119: Added line hit count to count column values (format: total / line in current Count column)..-122: Add option to only show x chars before/.after matched text..-12

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AstroGrep\AstroGrep.lnk	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Thu Apr 4 19:57:44 2019, mtime=Sun Jul 18 04:37:27 2021, atime=Thu Apr 4 19:57:44 2019, length=573440, window=hide
Category:	dropped
Size (bytes):	1110
Entropy (8bit):	4.634964714009965
Encrypted:	false
SSDEEP:	24:8mQzdPRmdOEop//OVlOUA7Ly5SdfmvdfvQUUtU7aB6m:8mcPRmdOrN/ClOj7Ly5SdfmvdfvFqxB6
MD5:	4E02F0D58593649DB109E42966511216
SHA1:	1F261578B7374A22C5727AFBA3CEDE9C8827990C
SHA-256:	9969E124D26F04D61C2BC62A9109C720B4826DF21EB92ADD4206FA52BE3B341B
SHA-512:	1CB19D3FF59E0A6773424B7CD5204F75BCCAE1A90D923F5E9A40E7381D12722A5480B68F65D731C6E18E167EC9FC7854F746DADD2ED6A67CAEB380603B5FD77
Malicious:	false
Preview:	L.....F.... .....).....i..{.....).....P.O. .:i.....+00.../C:\.....1.....>Qwx..PROGRA~2.....L..R.,.....V....._...P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....\.1.....R.,..ASTROG~1..D.....R.,.R.,.....Y.....E.A.s.t.r.o.G.r.e.p.....h.2.....N6. .ASTROG~1.EXE..L.....N6..R.,.....Y.....A.s.t.r.o.G.r.e.p...e.x.e.....]..-.....\.....%?t.....C:\Program Files (x86)\AstroGrep\AstroGrep.exe..=.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.A.s.t.r.o.G.r.e.p.\.A.s.t.r.o.G.r.e.p...e.x.e. .C.:\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.A.s.t.r.o.G.r.e.p.....*.....@Z|...K.J.....`.....X.....114127.....!a..%.H.VZAj...R..-.....-..!a..%.H.VZAj...R..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AstroGrep\Uninstall AstroGrep.lnk	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Sun Jul 18 04:37:27 2021, mtime=Sun Jul 18 04:37:27 2021, atime=Sun Jul 18 04:37:27 2021, length=61854, window=hide
Category:	dropped
Size (bytes):	1110

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AstroGrep\Uninstall AstroGrep.lnk	
Entropy (8bit):	4.665663359768743
Encrypted:	false
SSDEEP:	24:8m1aRvdOEopF/g+taHfUA7LMdfOhgdfvQUUKj7aB6m:8m1aRvdOrf/g+taHfj7LMdfOhgdfvFND
MD5:	F26EA75861C05D224B5375D6BF24E6FE
SHA1:	F21F56ADF6987A9A8E5A269817A4BC8574C78AF3
SHA-256:	BC15264E99D05B6459DEC01BBF8D55AEAD2E6CDBC166EE0578F217E350E3CA90
SHA-512:	9D5F1CFB1E8EF08D2D8F00D8F9B418C2AB820D09C417A50A1162F6029BA090D0E3A6D05AA1C313E152030D244520697D7BC4F3A5D5C9E73357BBA46A0E12625
Malicious:	false
Preview:	L.....F.... .....|..{...~..{...~..{.....P.O. .:i....+00.../C:\.....1.....R.,..PROGRA~2.....L..R.,.....V.....E[.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7....\.1.....R.,..ASTROG~1..D.....R.,.R.,.....Y.....tmC.A.s.t.r.o.G.r.e.p.....h.2.....R., .UNINST~1.EXE..L.....R.,.R.,.....Z.....9.A.U.n.i.n.s.t.a.l.l...e.x.e.....]...-.....\.....%?t.....C:\Program Files (x86)\AstroGrep\Uninstall.exe..=.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.A.s.t.r.o.G.r.e.p.\.U.n.i.n.s.t.a.l.l...e.x.e. .C.:\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.)\.A.s.t.r.o.G.r.e.p.....*.....@Z|...K.J.....`.....X.....114127.....!a..%.H.VZAj...q..-.....-..!a..%.H.VZAj...q..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ASTRO-GREP.EXE.log	
Process:	C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	614
Entropy (8bit):	5.330897468506462
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhaxzAbDLI4Mq92n4M6:ML9E4Ks2wKDE4KhK3VZ9pKhmsXE4x84j
MD5:	A4395C8F90A59E4CC7F7923D8BDE437C
SHA1:	A8E9EBD5CDF81E720979E795391EF2440CE5DA4A
SHA-256:	F84DFD4D4F8BA0113ED2C0394868B1E4C8F83850DE051FA599621098C190FE6E
SHA-512:	7F1F159667C7F4A9E60E272DF00A2D33A72816F35FEF1DAD37F17B089E506D1CCC0350D569690230F53A44DB49FFDB81BC6E47B7F96BB4469395926F3BC953D3
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	
Process:	C:\Users\user\Desktop\ms.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48640
Entropy (8bit):	5.561770945961325
Encrypted:	false
SSDEEP:	768:quCFNTAolrhWU5TeLmo2qrJW6K8e2gaM9PIltc5pIX0byDBm1ERjvmFq+YBDZsx:quCFNTA2G2d6K5aM6Itc5pIEbyAqRzyX
MD5:	432F0E0AAB658DE046D8B41D2CEF8253
SHA1:	7BA5B175FFB4BB976C54177F9C40A7339A088654
SHA-256:	17D1C0045155AD9C523C07E0F37AA16CD036915F38B73090D8D8BA930DB149FB
SHA-512:	BAC97805D8FCBA49B7BDE5067911B293622C610A65F2A2FC527A6C890BE8E79C6CA9C9676786B1EAAC19ECBDB16562EFEE2D7C985707FC04E57E4E3033C75E0B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^..... ....@.. ....@.....T...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....Y..Xv.....V..;...$0.xC.=VD..b.....9A../.\.....(....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*.:.:...(+...:...('..:.:...((...9....(v...*V(....s.... ...o....*n~....9....~....o.. .....*~~....(....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE	
Process:	C:\Users\user\Desktop\ms.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	950654
Entropy (8bit):	7.974042856320811
Encrypted:	false
SSDEEP:	24576:2MhCG3sDOdqnRrLVvjD9puJ7li2OLUC0Dc/rP0flxwg:AG3sJpRvjhU7I2OLZD/LUr7
MD5:	A708211241313FEAF9621E571631534D
SHA1:	9F398E0CC5B2B5162D5F27A6653709F836D02998
SHA-256:	5C4FAEBE335FEE04B25B10AA2A0E580571388BDE2CC09E133C72D9D01BC09423

C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE	
SHA-512:	8E2FA5F33E16879D8F5ACB4AB783AA4B4B37266CD1346ABEF5D54F2DFEB2177AF872575780E2E7CD02E462349B1C35642C0F7BA3F860034775A064E9A07B08A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...F...F...F.*.....F...G.v.F.*.....F..v...F...@...F.Rich..F..... .....PE..L....z.W.....`...|.....1.....p....@.....@.....4u.....pP.....p..... ....text...._.....`..... ..`.rdata..R....p.....d.....@..@.data....T.....x.....@....ndata.....rsrc...pP.....R...~.....@..@..... ....

C:\Users\user\AppData\Local\Temp\nsq211B.tmp\LangDLL.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	3.936685359308878
Encrypted:	false
SSDEEP:	48:im1qsjq8W2MPUptuMMFvx/om/ycNSCwVGfOY0vB6/JvR0Jvof5d2D:F1iBl91Z7/ycNSCwV8TLZR0gd2
MD5:	91D5E21907E4BAFF0145339311ABF9D9
SHA1:	F867D8529D4F3704CD4F475B46699B66CB6C2002
SHA-256:	ACDE373CC4916BE5DF3D239AB67F5980C333E979F34965EE733E7C6259586E9B
SHA-512:	339E35B89F2AC7D2FBE9DFD9A55279D20463F7C298332810C0EBAA5DE95E09657F4B2837904AE16A8743C4C7ABF7F3C7581099BC94312C178A21783288790401
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...}.}.}.}.e.....z.).....|....|.Rich}.....PE..L....z.W.....!..... ....`.....p"..I...` ..P....@..`.....P..... ..`.....text...h..... ..`.rda ta..... .....@..@.data...l....0.....@....rsrc...`....@.....@..@.reloc..l....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsq211B.tmp\StartMenu.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.616039420427882
Encrypted:	false
SSDEEP:	96:HgiqVPb3X8K8Kdr3gEq6nNdMk6Qiw290+q6LDtJ1tU3hhEl7y:HgiqVPgK8K9eIdE9B/tMhg7
MD5:	9CE20025DEF637F7BE257FA96D25ED05
SHA1:	CFEE47F72804FFACD06C2254A5F8DCF47373F9D4
SHA-256:	4B17C914DC40EBA477B653715F07CE9ED9B2EF4A1264A1DAFD624EB289474243
SHA-512:	AFCE99F1BD803E1B744E33302BA2C85C1122487F2BDF006CA433FE93DB2778A6D68D239D927CE7149443F411A12A4FAC2195D6D01AEC4071C71B8F332C96BDF B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I...(...(...(...(...(..<'...(.....(..8....(.....(..Rich.(.....PE.. L....z.W.....!.....".....p.....$..e.... ..x....P..(.....`..t..... .....text..... ..... ..`.rdata..U.... .....@..@.data.....0.....@....rsrc...(....P.....@..@.reloc..8....`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsq211B.tmp\System.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.770824470205811
Encrypted:	false
SSDEEP:	192:PPtkumJX7zB22kGwfy0mtVgkCPOs81un:E702k5qpds8Qn
MD5:	B8992E497D57001DDF100F9C397FCEF5
SHA1:	E26DDF101A2EC5027975D2909306457C6F61CFBD
SHA-256:	98BCD1DD88642F4DD36A300C76EBB1DDFBBBC5BFC7E3B6D7435DC6D6E030C13B
SHA-512:	8823B1904DCCFAF031068102CB1DEF7958A057F49FF369F0E061F1B4DB2090021AA620BB8442A2A6AC9355BB74EE54371DC2599C20DC723755A46EDE81533A3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....l....l.Richm.....PE..L....z.W.. .....!.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..... ..`.rdata..S....0.....".....@..@.data...h....@.....&.....@....reloc..`....P.....(.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsq211B.tmp\modern-wizard.bmp	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PC bitmap, Windows 3.x format, 164 x 314 x 4
Category:	dropped
Size (bytes):	52988
Entropy (8bit):	1.9568109962493656
Encrypted:	false
SSDEEP:	48:Qoi47a5G8SddzKFIcsOz3XMoi47a5G8SddzKFIcsOz3Xz:QonoGNd03IonoGNd03/
MD5:	E39731A71ED38499AC6B8E51E8E58E34
SHA1:	F2820C783906CD4F06040B6850856D426519CE15
SHA-256:	A94EF9A36E53192F26D5118F0232B6D7F70943B3CF5A7DF6340A139A226D207B
SHA-512:	F807ED5BE0297462777A82B79D1AAC35CB4FF5FA54DE4D446050A8BB08677488072685A982BFF5A900823C5727196C05EF29B3EEB6ABCD17171C0EF7C376527C
Malicious:	false
Preview:	BM~g......v...(.......:...........g...DDD@@@@DDDDDD@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@DDDDDDDDD@@@@DDDDDDDDD@@@@@@..DDD....DDDDDD.......................................DDDDDDDDDD....DDDDDDDDD........DD@@ @@DDDDDD@@DDDDDDDD@@@@DDDDDDDDDD@@@@@@@D.. DD....DDDDDDD.....................................DDDDDDDDDD....DDDDDDDDDD......D..D@@@@@DDDDDD@@@@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@DDDDDDDDDD@@@@DDDDDDDDDD@@@@@DDD..D.....DDDDDD.....................................DDDDDDDDD.....DDDDDDDDD......DDD ..@@@@@DDDDDD@@@DDDDDDDDD@@@@DDDDDDDDD@@@@@@ DDDD.......DDDDDD....................................DDDDDDDDDD....DDDDDDDDDD.....DDDDD..@@@@@DDDDDD@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@DDDDDDDDD@@@@DDDDDDDDD@@@@@@DDDDDD.......DDDDDD...................................DDDDDDDDD....DDDDDD DDDD......DDDDDD..@@@@DDDDDD@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

C:\Users\user\AppData\Local\Temp\nsq211B.tmp\nsDialogs.dll	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	5.066422293646434
Encrypted:	false
SSDEEP:	96:oU2qZ4zC5RH3cXX1LlYlRowycxM2DjDf3GEst+Nt+jvDYx4HpqndYHnxss:oU2q+CP3uKrpyREs06YxqodGn
MD5:	70D4C5F9ACC5DDF934B73FA311ADE7D8
SHA1:	6962E84782B0E1FE798CDCE1D7447211228CA85B
SHA-256:	02869B76936E3C3102BB36E34B41BC989770BF81DCA09F31C561BB6BE52285EE
SHA-512:	40189B463173CBBAD9C5101F37B4A37D970E9CD8E6F3D343CB8E54C54BDC7FDC3CFA8D7D7E7B7B0241C68768607C523BE2C2C21B7EFC727257731E1C5D1673 C
Malicious:	false
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......|..c8O`08O`08O`08Oa0.O`0.@=05O`0llP0=O`0.If09O`0.od0 9O`0Rich8O`0........PE..L....z.W...........!......... ...............0.......................................................................6..k....0.......`.......................p...0.. ....text...Q.......................... ..`.rdata..{....0......................@..@.data........@......................@....rsrc........`....... ....@..@.reloc..l....p......."..............@..B.. ....

C:\Users\user\AppData\Local\Temp\tmp7B21.tmp.bat	
Process:	C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	154
Entropy (8bit):	5.114193705430011
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViEaKC50XVASmqRDWXp5cViE2J5xAInTRI4XSu7ZPy:hWKqTtT6WXp+NaZ50lbmq1WXp+N23fT+
MD5:	005C284BFAC71599AEEDBFFA742E1D45
SHA1:	514D841D9D5C3A86E5A7AB8D77312156980F08E6
SHA-256:	B6D37A30E712121D18DE29C69F9289DB416F87298E031A9BCD103FF2EC8C2C87
SHA-512:	2A5FC7C31D1A62D638F4A8190573458AFF36F0DE37D392DEB932A5A46639475FDC1A9D29AD675B6F74301A5C2E2F4679B67B274313469248CFE312D743F90F6C
Malicious:	false
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Roaming\astro-grep.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmp7B21.tmp.bat" /f /q..

C:\Users\user\AppData\Roaming\astro-grep.exe	
Process:	C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48640
Entropy (8bit):	5.561770945961325
Encrypted:	false
SSDEEP:	768:quCFNTAolrhWU5TeLmo2qrJW6K8e2gaM9PIItc5pIX0byDBm1ERjvmFq+YBDZsx:quCFNTA2G2d6K5aM6Itc5pIEbyAqRzyX
MD5:	432F0E0AAB658DE046D8B41D2CEF8253

C:\Users\user\AppData\Roaming\astro-grep.exe	
SHA1:	7BA5B175FFB4BB976C54177F9C40A7339A088654
SHA-256:	17D1C0045155AD9C523C07E0F37AA16CD036915F38B73090D8D8BA930DB149FB
SHA-512:	BAC97805D8FCBA49B7BDE5067911B293622C610A65F2A2FC527A6C890BE8E79C6CA9C9676786B1EAAC19ECBDB16562EFEE2D7C985707FC04E57E4E3033C75E0B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\astro-grep.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^..... .....@.. ....@.....T...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....Y..Xv.....V..;...$0.xC.=VD..b.....9A../.\.....(....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*..:.....(+..:.....('..:.....((...9.....(v...*V(....s.... ...o....*n~....9....~....o.. .....*~~....(....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AAA4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.869948492165745
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ms.exe
File size:	1068032
MD5:	dbbb611daf3abd47972ae4faf5d54c95
SHA1:	1b33772f2acc9e6673a2922587b00db86f5fba01
SHA256:	d5a8b6cb7b39d6f71ce67c6c8e17030079f2778087ee12c0ad45bd823f7bd53c
SHA512:	140b2d0d6ac049943f5f2c8e3bfa7ca1ad773b0878cf92f825baa2769930d068b6b2601786f94f40daf15f199b2cb9b6ce6c016130025e5f04a103ee78b06bb9
SSDEEP:	24576:jmclmMhCG3sDOdqnRrLVvjD9puJ7li2OLUC0Dc/rP0flxwy:jmzG3sJpRvjhU7I2OLZD/LUr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..Q..... .....m.>.....m...F...m.....3.....V...m.....m.=.....Rich.... .....PE..L....0.N.....

File Icon

Icon Hash:	e0d08cf8d8ccc8e0

Static PE Info

General

Entrypoint:	0x403248
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x4E1030C0 [Sun Jul 3 09:05:04 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	9222d372923baed7aa9dfa28449a94ea

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x7842	0x7a00	False	0.589491547131	data	6.48776813349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x319e	0x3200	False	0.35390625	data	4.92389239742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd000	0x1a84	0xe00	False	0.215401785714	data	2.57332081688	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0xf78fc	0xf7a00	False	0.948167749874	data	7.91789788584	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x107000	0x13aa	0x1400	False	0.4107421875	data	4.12102642331	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 17, 2021 22:37:53.417326927 CEST	192.168.2.3	8.8.8.8	0xaf53	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 17, 2021 22:37:53.476236105 CEST	8.8.8.8	192.168.2.3	0xaf53	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jul 17, 2021 22:37:53.476236105 CEST	8.8.8.8	192.168.2.3	0xaf53	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 17, 2021 22:37:53.622780085 CEST	104.23.98.190	443	192.168.2.3	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 17 02:00:00 CEST 2021 Mon Jan 27 13:46:39 CET 2020	Sun Jul 17 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ms.exe PID: 4156 Parent PID: 5584

General

Start time:	22:36:58
Start date:	17/07/2021
Path:	C:\Users\user\Desktop\ms.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ms.exe'
Imagebase:	0xa30000
File size:	1068032 bytes

MD5 hash:	DBBB611DAF3ABD47972AE4FAF5D54C95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000001.00000002.200014509.0000000000A3F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000001.00000000.195464436.0000000000A3F000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Analysis Process: ASTRO-GREP.EXE PID: 5416 Parent PID: 4156

General

Start time:	22:37:00
Start date:	17/07/2021
Path:	C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE'
Imagebase:	0x5f0000
File size:	48640 bytes
MD5 hash:	432F0E0AAB658DE046D8B41D2CEF8253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.250713765.0000000002A4E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000000.197769647.00000000005F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.250001680.00000000005F2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: ASTROGREP_SETUP_V4.4.7.EXE PID: 3728 Parent PID: 4156

General

Start time:	22:37:00
Start date:	17/07/2021
Path:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE'
Imagebase:	0x400000
File size:	950654 bytes
MD5 hash:	A708211241313FEAF9621E571631534D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 4%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 912 Parent PID: 5416

General

Start time:	22:37:23
Start date:	17/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c schtasks /create /f /sc onlogon /rl highest /tn 'astro-grep' /tr "C:\Users\user\AppData\Roaming\astro-grep.exe" & exit
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3820 Parent PID: 912

General

Start time:	22:37:24
Start date:	17/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 3352 Parent PID: 5416

General

Start time:	22:37:24
Start date:	17/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\tmp7B21.tmp.bat"
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 784 Parent PID: 3352

General

Start time:	22:37:24
Start date:	17/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5996 Parent PID: 912

General

Start time:	22:37:24
Start date:	17/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn 'astro-grep' /tr ''C:\Users\user\AppData\Roaming\astro-grep.exe''
Imagebase:	0xcb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: timeout.exe PID: 1364 Parent PID: 3352

General

Start time:	22:37:25
Start date:	17/07/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x1020000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

Analysis Process: astro-grep.exe PID: 748 Parent PID: 528

General

Start time:	22:37:25
Start date:	17/07/2021
Path:	C:\Users\user\AppData\Roaming\astro-grep.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\astro-grep.exe
Imagebase:	0x770000
File size:	48640 bytes
MD5 hash:	432F0E0AAB658DE046D8B41D2CEF8253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000D.00000000.253043295.0000000000772000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000D.00000002.460832273.0000000000772000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\astro-grep.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Analysis Process: astro-grep.exe PID: 2792 Parent PID: 3352

General

Start time:	22:37:29
Start date:	17/07/2021
Path:	C:\Users\user\AppData\Roaming\astro-grep.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\astro-grep.exe'
Imagebase:	0x430000
File size:	48640 bytes
MD5 hash:	432F0E0AAB658DE046D8B41D2CEF8253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000002.310239259.0000000000432000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000000.259955019.0000000000432000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis