ID: 450275
Sample Name: astro-grep-setup.exe.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:39:14
Date: 17/07/2021
Version: 33.0.0 White Diamond

Table of Contents

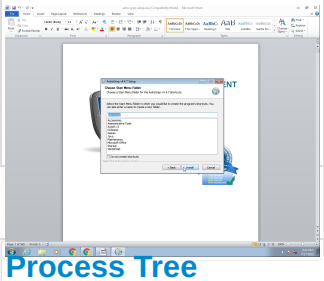
Windows Analysis Report astro-grep-setup.exe.doc

Overview

General Information

Sample Name:	astro-grep-setup.exe.doc
Analysis ID:	450275
MD5:	9c3d3679ea84ff9..
SHA1:	0470d616e8918e..
SHA256:	2f5639932c7a25c..
Tags:	AstroGrep doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

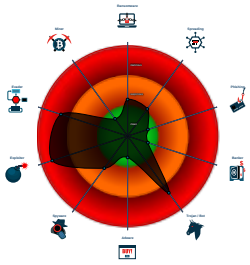
AsyncRAT

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

Signatures

- Antivirus detection for dropped file
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected AsyncRAT
- .NET source code contains potentia…
- Connects to a pastebin service (like…
- Contains functionality to check if a d…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2788 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - ms.exe (PID: 1260 cmdline: C:\ProgramData\Memsys\ms.exe MD5: DBBB611DAF3ABD47972AE4FAF5D54C95)
    - ASTRO-GREP.EXE (PID: 2432 cmdline: 'C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE' MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
      - cmd.exe (PID: 1784 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: AD7B9C14083B52BC532FBA5948342B98)
        - schtasks.exe (PID: 2220 cmdline: schtasks /create /f /sc onlogon /rl highest /tn 'astro-grep' /tr "C:\Users\user\AppData\Roaming\astro-grep.exe" MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - cmd.exe (PID: 1068 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\tmp3E29.tmp.bat" MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2288 cmdline: timeout 3 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
        - astro-grep.exe (PID: 1428 cmdline: 'C:\Users\user\AppData\Roaming\astro-grep.exe' MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
    - ASTROGREP_SETUP_V4.4.7.EXE (PID: 2328 cmdline: 'C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE' MD5: A708211241313FEAF9621E571631534D)
- taskeng.exe (PID: 2320 cmdline: taskeng.exe {E0184388-4CC0-4E79-AF38-011207705295} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - astro-grep.exe (PID: 2468 cmdline: C:\Users\user\AppData\Roaming\astro-grep.exe MD5: 432F0E0AAB658DE046D8B41D2CEF8253)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

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

Source	Rule	Description	Author	Strings
C:\ProgramData\Memsys\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
C:\ProgramData\Memsys\ms.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.2441547401.0000000000922000.00000020.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000C.00000000.2447425472.000000000192000.00000020.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000000.2450569517.000000000192000.00000020.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000002.2501813179.000000000192000.00000020.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000003.00000000.2389222840.0000000000922000.00000020.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.astro-grep.exe.190000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.ASTRO-GREP.EXE.920000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
14.0.astro-grep.exe.190000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.ASTRO-GREP.EXE.24afcd8.1.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
12.0.astro-grep.exe.190000.0.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 detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with base64 encoded strings

Document contains an embedded VBA with hexadecimal encoded strings

Office process drops PE file

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:

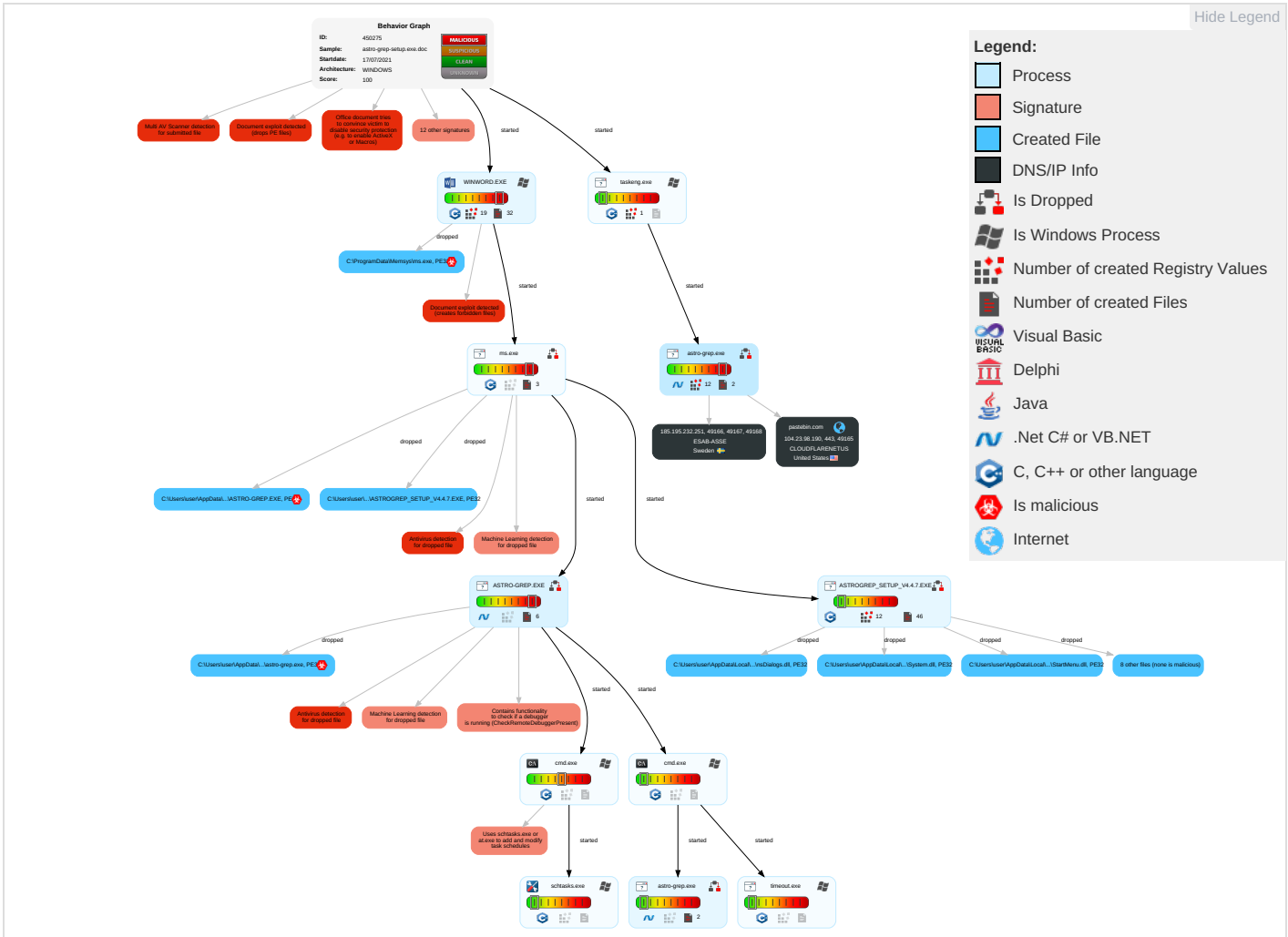
Yara detected AsyncRAT

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	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1	Eavesdr Insecure Network Commu
Default Accounts	Scripting 4 2 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Scripting 4 2 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirec Calls/SM
Domain Accounts	Native API 1	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 1 1 1	Security Account Manager	System Information Discovery 2 7	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Encrypted Channel 1 2	Exploit S Track D Locatior

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Scheduled Task/Job 2	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Standard Port 1	SIM Car Swap
Cloud Accounts	Command and Scripting Interpreter 3	Network Logon Script	Registry Run Keys / Startup Folder 1	Extra Window Memory Injection 1	LSA Secrets	Security Software Discovery 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipul Device Commu
Replication Through Removable Media	Scheduled Task/Job 2	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4 1	DCSync	Virtualization/Sandbox Evasion 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

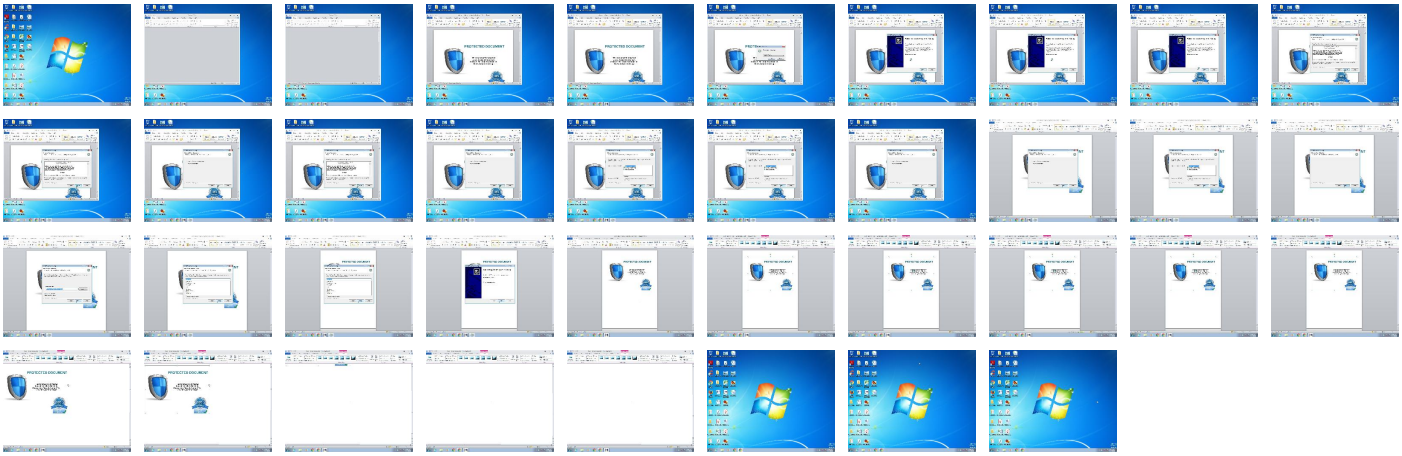
Behavior Graph

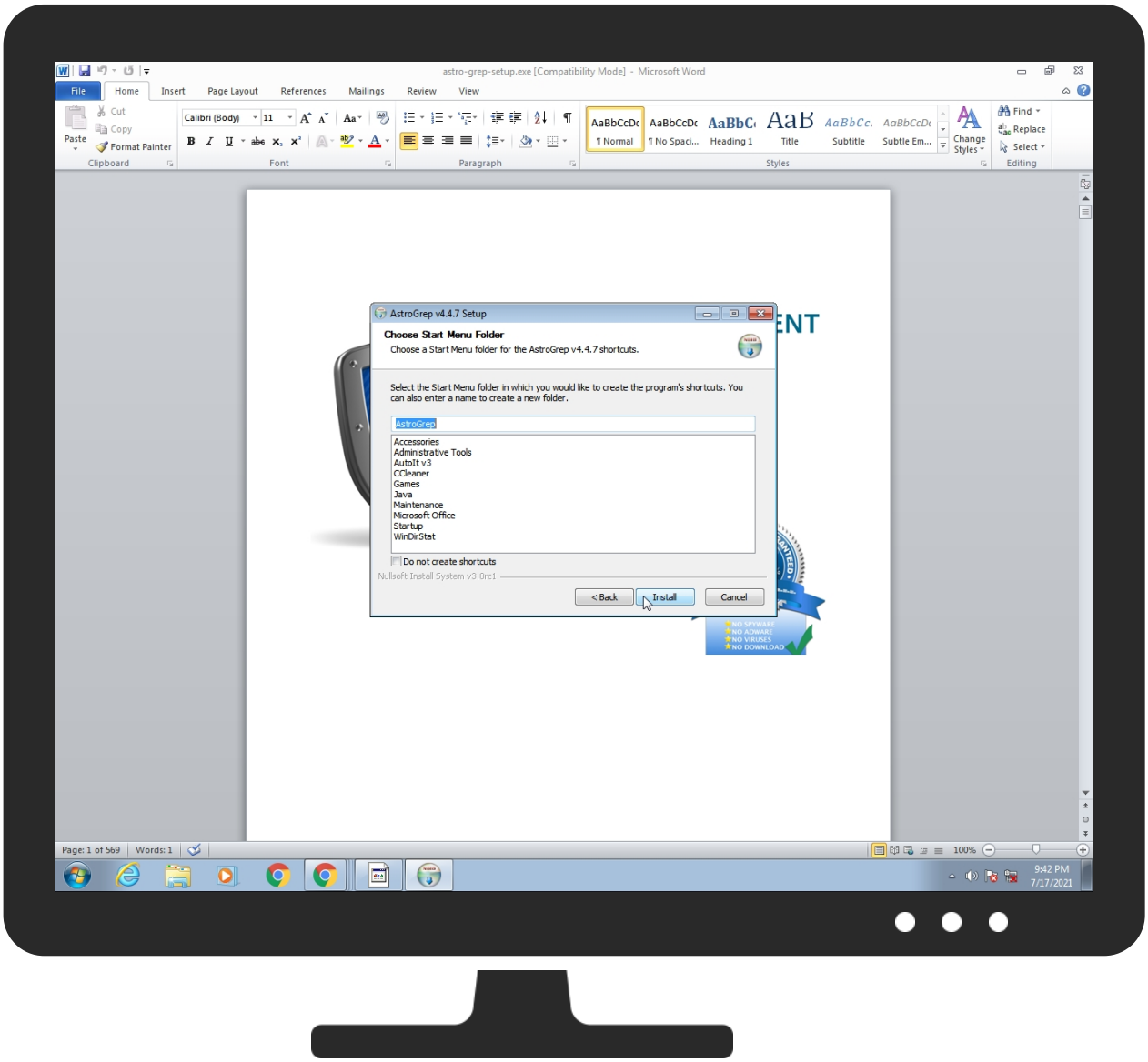


Screenshots

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
astro-grep-setup.exe.doc	60%	Virustotal		Browse
astro-grep-setup.exe.doc	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:\ProgramData\Memsys\ms.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:\ProgramData\Memsys\ms.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%	Virustotal		Browse
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	1%	Virustotal		Browse
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
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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.astro-grep.exe.190000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.astro-grep.exe.190000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.ASTRO-GREP.EXE.920000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.0.ms.exe.b8b130.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.astro-grep.exe.190000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.2.ms.exe.b70000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.2.astro-grep.exe.190000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.0.ASTRO-GREP.EXE.920000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.ASTRO-GREP.EXE.24afcd8.1.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
2.0.ms.exe.b70000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.2.ms.exe.b8b130.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://pastebin.comP	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	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:	450275
Start date:	17.07.2021
Start time:	21:39:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	astro-grep-setup.exe.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	15
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@20/36@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 48.5% (good quality ratio 41.8%) • Quality average: 72.3% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:42:01	API Interceptor	9x Sleep call for process: ms.exe modified
21:42:02	API Interceptor	342x Sleep call for process: ASTROGREP_SETUP_V4.4.7.EXE modified
21:42:02	API Interceptor	213x Sleep call for process: ASTRO-GREP.EXE modified
21:42:26	API Interceptor	2x Sleep call for process: schtasks.exe modified
21:42:28	Task Scheduler	Run new task: astro-grep path: "C:\Users\user\AppData\Roaming\astro-grep.exe"
21:42:28	API Interceptor	427x Sleep call for process: taskeng.exe modified
21:42:29	API Interceptor	401x Sleep call for process: astro-grep.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.195.232.251	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
	EU441789083.doc	Get hash	malicious	Browse	• pastebin.com/raw/BCAJ8TgJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	1KITgJnGbI.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	TIJYYIYJpv.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
	G-DECL G50 EURL.xlsx	Get hash	malicious	Browse	• 104.23.99.190
	C1jT7pIYSJ.exe	Get hash	malicious	Browse	• 104.23.98.190
	7NBeM7iVOm.exe	Get hash	malicious	Browse	• 104.23.98.190

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	UwvHsxxITi.exe	Get hash	malicious	Browse	• 104.21.19.209
	gVI2IrBzjJ.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
	banload.msi	Get hash	malicious	Browse	• 104.23.99.190
ESAB-ASSE	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
	S22NFM14.exe	Get hash	malicious	Browse	• 185.65.135.254

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	Order Request.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	product list.doc	Get hash	malicious	Browse	• 104.23.98.190
	KV18RE001-A5193.doc	Get hash	malicious	Browse	• 104.23.98.190
	ABS 1234 PO.docx	Get hash	malicious	Browse	• 104.23.98.190
	REQUIREMENT-DWG-454888_2021.doc	Get hash	malicious	Browse	• 104.23.98.190
	purchase order.doc	Get hash	malicious	Browse	• 104.23.98.190
	lokibot.docx	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-21213.docx	Get hash	malicious	Browse	• 104.23.98.190
	New Order 5678.doc	Get hash	malicious	Browse	• 104.23.98.190
	RFQ 110739914MCH.doc	Get hash	malicious	Browse	• 104.23.98.190
	6171557.docm	Get hash	malicious	Browse	• 104.23.98.190
	6171557.docm	Get hash	malicious	Browse	• 104.23.98.190
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	nanomalware.doc	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ETL_5100006278946.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	01130100370.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	IMG_056029741000.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	LL52387-01M4205301.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	Outfordelivery389402.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	LL52387-01-F4448869.xlsm	Get hash	malicious	Browse	• 104.23.98.190

Dropped Files

No context

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%
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
SHA-512:	A054A7FD69E4A643286212FEDABDE4BDFB36BBF3E7F9FC33524BA8DFECBC375E991C23B4E047F5F235A77E9D6A525F996934A4A993B61E1FE7D84066FF972D 1
Malicious:	false
Reputation:	low
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

C:\Program Files (x86)\AstroGrep\AstroGrep.Common.dll	
MD5:	2F2899673ABB136BFC8B92A6D3BAFF33
SHA1:	5BE14D5C58AF9F78858DD5E9ED6CD929F87AC0B4
SHA-256:	0E7A71232FB6676777A823ADDB4776BD895ABBE29EA2487110073BD0C5FF6AA6
SHA-512:	CF5B23F4E5417DDC4AB5A354E7EA90C5CCE28133DE7D1AE260F0879E474727DBB73E47C9CB92A98BD5B6F6EBCFC67CD955423FA1615A0D7C24783415325200A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
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: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 0%
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:	EBA2DD5216BB3293BB3101A5CDADDEF0B4A94577159A8A0654F712F9939F1D03FF670DA6DF0B5F4475D593EDDF330E76E2F6EB19B19E3E51C2EA53A74ACC59B3
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

C:\Program Files (x86)\AstroGrep\AstroGrep_256x256.png	
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%
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%
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

C:\Program Files (x86)\AstroGrep\Uninstall.exe	
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 Documents..-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\Memsys\ms.exe	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	174144
Entropy (8bit):	6.491457088878327
Encrypted:	false
SSDEEP:	3072:tMSncRzAOjuCDTA2G2dBOItczBbyjGUOx2w4gnScG4DI2dcP456WN3cahj:uSncRljuCfzd3tczBb7292+MN3cKj
MD5:	2BD7A81D9DC6F3D44FD977580271C1F1
SHA1:	A698930115AD68DDC1471C0F66EDB1E6F913B468
SHA-256:	43DEC507E474ECA562BE1D6329A842ECD8A7A68E8EF0BA2E3EB8033C1CF18CEA
SHA-512:	7494DB34B4E2E2D6A4F92E22DDCD2CAEB296A27BF6E5544CB29C99ABDA51DB9B52676DDDA39ED44B570E9A7816C65F1976F40008BECCE5FA4F8B341B0722ABBE
Malicious:	**true**
Yara Hits:	• Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\ProgramData\Memsys\ms.exe, Author: Florian Roth • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\ProgramData\Memsys\ms.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....$.....F..Q.....m.>.....m...F...m.....3.....V...m.....m.=.....Rich.....PE..L....0.N.....z.....H2.....@.....Z....@.....<.....x.....p.....`.....H...@.....$.....text...Bx.....z..... ..`.rdata...1.....2...~.....@..@.data.....@....rsrc....x.....z.....@..@.reloc.....p.....8.....@..B

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 03:42:39 2021, atime=Thu Apr 4 19:57:44 2019, length=573440, window=hide
Category:	dropped
Size (bytes):	1037
Entropy (8bit):	4.527784755515661
Encrypted:	false
SSDEEP:	24:8mQ50FJcdOEv+ZYF/iVgcN6OUA1Ly5Sdfmvdfv8U53qod7y:8mDidO/+/GrN6Oj1Ly5SdfmvdfvpAoxy
MD5:	D50C2DC45DA94A42EB3519FFB9ECDFB5
SHA1:	EF70BADE52AE9C1DE9B21EAE6E73958C62D26A81
SHA-256:	37D91F7E68DC5F1C9ECA21659628748A6F6EF525E5B8C383DD56F4E86440A8C5
SHA-512:	FF649AE63C9E45182C710CA38230C8E3ADAFEA489939051C8A53C591AC8D0BD763509FA84F64AFDA0233BB13588BEBC9E5AE0F34F9CD6F9611B84DB6F985470
Malicious:	false
Preview:	L.....F.... .....).....V.{.....).....P.O. .:i.....+00.../C:\.....1.....RT%..PROGRA~2..|.....:...RT%*.....R.....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.....X.1.....RU%..ASTROG~1..@.....RT%.RU%*...Y.....A.s.t.r.o.G.r.e.p.....d.2.....N6. .ASTROG~1.EXE..H.....N6..RT%*...'.....A.s.t.r.o.G.r.e.p...e.x.e.....]..... -.....\.....ah.H.....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.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....715575.....D_....3N...W...9M.C.....

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AstroGrep\Uninstall AstroGrep.lnk	
Process:	C:\Users\user\AppData\Local\Temp\ASTROGREP_SETUP_V4.4.7.EXE

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AstroGrep\Uninstall AstroGrep.lnk	
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 03:42:40 2021, mtime=Sun Jul 18 03:42:40 2021, atime=Sun Jul 18 03:42:40 2021, length=61854, window=hide
Category:	dropped
Size (bytes):	1037
Entropy (8bit):	4.53537478019611
Encrypted:	false
SSDEEP:	24:8mTJcdOEv+ZYF/8lcafUA1LMdfOhgdfv8U53qoi7n:8mTidO/+/8+afj1LMdfOhgdfvpAoIn
MD5:	C36F8465E6054E0FCCF8AA35BF1EB274
SHA1:	623D0C3FE44A45160A6323052813DF2E41AE8950
SHA-256:	6BC551B7116E1F41183A6A1F1AB103C4202E0F5317F15AFF6D99BE41CB406E7C
SHA-512:	CBD28E78DC0E1011A462651C852812FFADCC9E2390D940992CBDA4146E12DC76082023498422F2ECD297738BB1CFF825275C1AA1A9C6087FA59394D9C6F6D0E
Malicious:	false
Preview:	L..................F.... ....%.W.{...%.W.{...%.W.{...............................P.O. .:i.....+00.../C:\.....................1......RT%..PROGRA~2..|.......:...RT%*...................R.....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.....X.1......RU%..ASTROG~1..@.......RT%.RU%*...Y....................A.s.t.r.o.G.r.e.p.....d.2......RU% .UNINST~1.EXE..H.... ...RU%.RU%*........................U.n.i.n.s.t.a.l.l...e.x.e.......]..............-.......\..........ah.H.....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.....................1SPS.XF.L8C... .&.m.m............-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6............`.......X.......715575..........D_....3N...W...9N.C...........

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78FF0AD.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1024 x 768, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	297570
Entropy (8bit):	7.987371833942709
Encrypted:	false
SSDEEP:	6144:wM9q9mzZATahSx65T341zP0LFDPV1W0ilwn8/aaT2J/3Qw9t69Im1J3G:1q90ZATahIMPLVKwCm/3QwKTu
MD5:	59AC9BE84B9A41DC7BA9B4CC0DC0B2BE
SHA1:	2F3958FC9B12179EF4003D215D6B609C4B387C95
SHA-256:	B094944CDD0D7F55FF67CAC98C150C59F67D27A60E661CF403C21D3E22CA4C50
SHA-512:	7FE0BD9AD21A3201F2A056802BE55C48251DA44D66B8D50D1843E47C25C1C92D272827EF2C26D3EBEF187F215BF07F9C71433FFC68FF0E2A0A9E609E05E7C34
Malicious:	false
Preview:	.PNG........IHDR.....................bKGD.............pHYs................tIME......1(.p.....iTXtComment.....Created with GIMPd.e... .IDATx...y`.g}7..3..,.lY.$.....9..$%$...B8J.@.........@ K.i)....H.B........q|.G,...[.{g.y..se.......A.......X.....#...DDDDDDDtJSx.......... """"""""&..........""""""""b.......... """"""""&..........""""""""b..........""""""""b.......... """"""""&..........""""""""b.......... """"""""&.......... """"""""&..........""""""""b.......... """"""""&..........""""""""b..........""""""""b.......... """"""""&..........""""""""b.......... """"""""&..........""""""""&..........""""""""b.......... """"""""&......... ..""""""""b.......... """"""""b.......... """"""""&..........""""""""b.......... """"""""&..........""""""""&..........""""""""b.......... """"""""&..........""""""""b.......... """"""""&.......... """"""""&..........""""""""b.......... """"""""&..........""""""""b..........""""""""b.......... """"""""&..........""""""""b.......... """"""""&.......... """"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5BCB44D4-31CD-44E2-A821-3408DFB7CA1A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.1215386864328073
Encrypted:	false
SSDEEP:	3:JlXll/lGNWtWlxlG:ANyiC
MD5:	6D00E84E5EDAA43E119EA03CE5ECAA4F
SHA1:	9FA7D5D09FED0A7C1F8392022EAAA24B66F4E77B
SHA-256:	957DA89085D8855135307E641A71C5EA2284BE478C115D7A6C3E9C095E83D407
SHA-512:	9DD9AD771F98A2AA72A238FCFE2F34AE181059A55A214A0B3EF7238916E9494B7BE5510DF0884B1CB1D357578E27F0E9B13F5CB7A1002E4583DBF428D3BBA0BE
Malicious:	false
Preview:	D...D.d...D...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8DB8CC3B-9141-43B7-951A-41190F623D30}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4273664
Entropy (8bit):	2.9934039252196754
Encrypted:	false
SSDEEP:	3072:asEquQFSZO2fZBlq5KsmqL15nSLK42srUUNoBbTTShbliRWMTwHh2ABRSDxnj/gH:G
MD5:	204EB5AEA47FB729502B517C7FEEF002
SHA1:	8AFE0FC7C7C994683ECE60B4E97325A96E5D66A0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8DB8CC3B-9141-43B7-951A-41190F623D30}.tmp	
SHA-256:	6A83F0B564303E74D593CB04D9845BE911367173011C27DD1A23771004C3E43B
SHA-512:	3458DDB5F132361EF9F919BD2FB8E1490ACF911090E7B8B3DE623821CA4058EA36E8FDAB03D3C8F1D5649CF26C230CC098DDCB190AFFA77C06335FB5F20419 8
Malicious:	false
Preview:	../..... ...."...$...&...(...*...,.....0...2..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{90768F62-679A-419C-A2B1-C0B28319F5E4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FBF58E38-2270-4D70-A99C-79301888F689}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.357318797251612
Encrypted:	false
SSDEEP:	3:Iiiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb5:Iiiiiiiiifdlloz Qc8++IsJe1MzG
MD5:	725A361F060B89059A926A98B5426871
SHA1:	3F5DF773068BB7382415782D3A0C4A8B1E7666D5
SHA-256:	A0F0BE63E9A1345B9D5FC8BBD74FF0CF238B1C56BACED75257F606F5EDAE3360
SHA-512:	2888DBF1D2341A033F691050C8A8204BB1C849894433DD3AA5C4CF41F8F74B04229560B4BC465082C9E312A0963D86F4971B5B1CCCED279CFCAECAA407E8F0E
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	
Process:	C:\ProgramData\Memsys\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:quCFNTAolrhWU5TeLmo2qrJW6K8e2gaM9PIItc5pIX0byDBm1ERjvmFq+YBDZsx:quCFNTA2G2d6K5aM6Itc5pIEbyAqRzyX
MD5:	432F0E0AAB658DE046D8B41D2CEF8253
SHA1:	7BA5B175FFB4BB976C54177F9C40A7339A088654
SHA-256:	17D1C0045155AD9C523C07E0F37AA16CD036915F38B73090D8D8BA930DB149FB
SHA-512:	BAC97805D8FCBA49B7BDE5067911B293622C610A65F2A2FC527A6C890BE8E79C6CA9C9676786B1EAAC19ECBDB16562EFEE2D7C985707FC04E57E4E3033C75E 0B
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%

C:\Users\user\AppData\Local\Temp\ASTRO-GREP.EXE	
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:\ProgramData\Memsys\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:AG3sJpRvjhU7l2OLZD/LUr7
MD5:	A708211241313FEAF9621E571631534D
SHA1:	9F398E0CC5B2B5162D5F27A6653709F836D02998
SHA-256:	5C4FAEBE335FEE04B25B10AA2A0E580571388BDE2CC09E133C72D9D01BC09423
SHA-512:	8E2FA5F33E16879D8F5ACB4AB783AA4B4B37266CD1346ABEF5D54F2DFEB2177AF872575780E2E7CD02E462349B1C35642C0F7BA3F860034775A064E9A07B08A
Malicious:	false
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\msoB754.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
Malicious:	false
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'.;..b...RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR..*.++..... ....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Local\Temp\nsa2731.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\nsa2731.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

C:\Users\user\AppData\Local\Temp\nsa2731.tmp\StartMenu.dll	
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\nsa2731.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:	8823B1904DCCFAF031068102CB1DEF7958A057F49FF369F0E061F1B4DB2090021AA620BB8442A2A6AC9355BB74EE54371DC2599C20DC723755A46EDE81533A3C
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\nsa2731.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@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@DDDDDDDDDD@@@@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@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@DDDDDDDDDD@@@@DDDDDDDDD@@@@@@@DDDDDD.......DDDDDD...................................DDDDDDDDD....DDDDDD DDDD......DDDDDD..@@@@DDDDDD@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

C:\Users\user\AppData\Local\Temp\nsa2731.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

C:\Users\user\AppData\Local\Temp\nsa2731.tmp\nsDialogs.dll	
SHA-256:	02869B76936E3C3102BB36E34B41BC989770BF81DCA09F31C561BB6BE52285EE
SHA-512:	40189B463173CBBAD9C5101F37B4A37D970E9CD8E6F3D343CB8E54C54BDC7FDC3CFA8D7D7E7B7B0241C68768607C523BE2C2C21B7EFC727257731E1C5D167 C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|..c8O`08O`08O`08Oa0.O`0.@=05O`0llP0=O`0.lf09O`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\tmp3E29.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):	5.06434100410945
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oXp4EaKC50XVASmqRDXp4E2J5xAlnTRI8TRAVZPy:hWKqTtT6PaZ50lbmq1P23fTddAVk
MD5:	71BD5BD91EBB91A939E0AB0D6560D28C
SHA1:	79CB69D678C58EF3122EC81443DB4D38AF084106
SHA-256:	227660DC691F3F47674D8F2DBCC48DF47B90F59D3E44092285999F170B9C1BFB
SHA-512:	F73C85CABA1A8719B35C3691833A8F2A609177461AB600323F87D1E8B234426F2FD32E2CC44876D642369AE5814A8F5C978EFE150D32A2EB434D911BBD2EA543
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 "tmp3E29.tmp.bat" /f /q..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\astro-grep-setup.exe.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Sun Jul 18 03:39:30 2021, length=1443117, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.541182450687829
Encrypted:	false
SSDEEP:	48:8i/XT3Ikt31S733oQh2i/XT3Ikt31S733oQ/:8i/XLIkt8noQh2i/XLIkt8noQ/
MD5:	5AD95C6B24A9E0814C973A7DD0152BCB
SHA1:	2D64590D05D4F190A646F9FAF93029097ACE7FD9
SHA-256:	C5DACC366D0349956C96DBE0661C0ACA8403D721A62AECB7A77C51E2FC5A6655
SHA-512:	6A960C8EA7646BCF890511D851FCC47D3B4AC76EEC06DEF2B1F6C3D0F450410EC16FB78D006F554DDD74325BF2CB242AFC99D1EF14213D0CCD8DC0E5CBE8 C0
Malicious:	false
Preview:	L.....F.... ...8N/..{..8N/..{...t..{..-.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....z.2.-.....R.$ .ASTRO-~1.DOC..^.....Q.y.Q.y*...8.....a.s.t.r.o.-.g.r.e.p.-.s.e.t.u.p...e.x.e...d.o.c.....-...8...[.....?J.....C:\Users\..#..... .\\715575\Users.user\Desktop\astro-grep-setup.exe.doc./.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.s.t.r.o.-.g.r.e.p.-.s.e.t.u.p...e.x.e...d.o.c.....:.,.LB.)...Ag.....1SP S.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....715575.....D_..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	98
Entropy (8bit):	4.352453630060136
Encrypted:	false
SSDEEP:	3:M1ZXOXPAkup2cWMXPAkup2mX1ZXOXPAkup2v:MGfAkefAknfAkd
MD5:	FD515263006BC00A3695B759289A747D
SHA1:	7CFDEC2A9BC2784996AC6D9DC6A0E0DEBD95E289
SHA-256:	E7834A7517ACADC1A45332C2B9BDF1024E0B4830370ED8B9CCB3AD77FA3B7F7A
SHA-512:	0ACDE3E772B32919F76188A0B8BDCF216DCC9B356D481E1DAE417C18DB4E361493B15FC0A4A9323020E508A71081C491DF5DC4EF76C25AB6089237688678DF2
Malicious:	false
Preview:	[doc]..astro-grep-setup.exe.LNK=0..astro-grep-setup.exe.LNK=0..[doc]..astro-grep-setup.exe.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

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
SHA1:	7BA5B175FFB4BB976C54177F9C40A7339A088654
SHA-256:	17D1C0045155AD9C523C07E0F37AA16CD036915F38B73090D8D8BA930DB149FB
SHA-512:	BAC97805D8FCBA49B7BDE5067911B293622C610A65F2A2FC527A6C890BE8E79C6CA9C9676786B1EAAC19ECBDB16562EFEE2D7C985707FC04E57E4E3033C75E 0B
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...

C:\Users\user\Desktop\~$tro-grep-setup.exe.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

\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:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AA A4
Malicious:	false

\Device\Null	
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.994288640917192
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 86.67% • ZIP compressed archive (8000/1) 13.33%
File name:	astro-grep-setup.exe.doc
File size:	1446736
MD5:	9c3d3679ea84ff9bf67bf8c7aa2afc48
SHA1:	0470d616e8918ef03098741bf7fb0b313bb8aaea
SHA256:	2f5639932c7a25cf51737748cdc495367a9203e0a963f930f0009935109da190
SHA512:	6896ad9abbbaa7760825d40086270f649a82a1291798173764e20deb7a5ef7a2f4070e247f27210f77341d70b6ed7215fa72a1711210610b428fcce39006af53
SSDEEP:	24576:gbi5q1lXj0di8tpgg/d3EVxW5Y62ddfMqKFIqlzFOQ1Yq8X2LcDLN:gbi5q1lXPupgU8Wy62dJVhqUYYq8X2s
File Content Preview:	PK.....!.....[Content_Types].xml.UKo.1..W.?.|.b...B....#T"H\g...._.'i...'..B...^V.....6.....Wr**.:../k.u.q.^T...`..Zl1.....b.1W....+..A..W. ...s.....kZ.....N.....n.....?..4...f..H..b.F.qYm|+]...3.....&...E.....b.|g.g

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/450275/sample/astro-grep-setup.exe.doc"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Streams with VBA

Streams

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 21:43:22.421515942 CEST	192.168.2.22	8.8.8.8	0x919c	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 21:43:22.482573986 CEST	8.8.8.8	192.168.2.22	0x919c	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Jul 17, 2021 21:43:22.482573986 CEST	8.8.8.8	192.168.2.22	0x919c	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 21:43:23.080955982 CEST	104.23.98.190	443	192.168.2.22	49165	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	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					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: WINWORD.EXE PID: 2788 Parent PID: 584

General

Start time:	21:39:30
Start date:	17/07/2021

Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13ff90000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Modified

Analysis Process: ms.exe PID: 1260 Parent PID: 2788

General

Start time:	21:42:00
Start date:	17/07/2021
Path:	C:\ProgramData\Memsys\ms.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Memsys\ms.exe
Imagebase:	0xb70000
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: 00000002.00000002.2391184390.0000000000B7F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000002.00000000.2386988323.0000000000B7F000.00000002.00020000.sdmp, Author: Joe Security • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\ProgramData\Memsys\ms.exe, Author: Florian Roth • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\ProgramData\Memsys\ms.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

Analysis Process: ASTRO-GREP.EXE PID: 2432 Parent PID: 1260

General

Start time:	21:42:01
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:	0x920000
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: 00000003.00000002.2441547401.0000000000922000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000000.2389222840.0000000000922000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.2441758985.00000000024AF000.00000004.00000001.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: 2328 Parent PID: 1260

General

Start time:	21:42:02
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
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: 1784 Parent PID: 2432

General

Start time:	21:42:25
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:	0x4a680000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: cmd.exe PID: 1068 Parent PID: 2432

General

Start time:	21:42:25
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\tmp3E29.tmp.bat"
Imagebase:	0x4a680000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Deleted

File Read

Analysis Process: schtasks.exe PID: 2220 Parent PID: 1784

General

Start time:	21:42:26

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:	0x9f0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 2288 Parent PID: 1068

General

Start time:	21:42:26
Start date:	17/07/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x270000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Analysis Process: taskeng.exe PID: 2320 Parent PID: 860

General

Start time:	21:42:28
Start date:	17/07/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {E0184388-4CC0-4E79-AF38-011207705295} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xfff50000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: astro-grep.exe PID: 2468 Parent PID: 2320

General

Start time:	21:42:28
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:	0x190000
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: 0000000C.00000000.2447425472.0000000000192000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000C.00000002.2652015747.0000000000192000.00000020.00020000.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 Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: astro-grep.exe PID: 1428 Parent PID: 1068

General

Start time:	21:42:30
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:	0x190000
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: 0000000E.00000000.2450569517.0000000000192000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000002.2501813179.0000000000192000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis