ID: 1280109
Sample Name: 15e7232gfN.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:59:55
Date: 26/07/2023
Version: 38.0.0 Beryl

Table of Contents

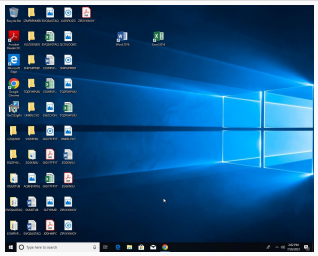
Windows Analysis Report

15e7232gfN.msi

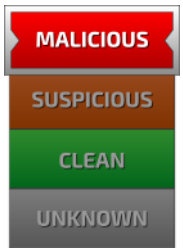
Overview

General Information

Sample Name:	15e7232gfN.msi
Original Sample Name:	6e068b9dcd8d…
Analysis ID:	1280109
MD5:	247a8cc39384…
SHA1:	23893f035f856…
SHA256:	6e068b9dcd8d…
Infos:	



Detection

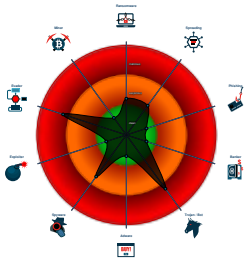


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dom…
- Connects to many ports of the same…
- Tries to detect sandboxes and other…
- Uses known network protocols on n…
- Creates a thread in another existing…
- Queries the volume information (nam…
- Drops PE files to the application pro…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 7028 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\15e7232gfN.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 4764 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 7100 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding D8DD1A2B41DAA758FA08D3E85077DC6F MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 7068 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 5484 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 6052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Autoit3.exe (PID: 4108 cmdline: "C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe" UGtZgHHT.au3 MD5: C56B5F0201A3B3DE53E561FE76912BFD)
      - cmd.exe (PID: 4696 cmdline: cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - OLicenseHeartbeat.exe (PID: 3132 cmdline: C:\Program Files (x86)\common files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe MD5: CFD37109A4E595C2957C5E0ACC198E8A)
    - icacls.exe (PID: 6980 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 4952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Autoit3.exe (PID: 7204 cmdline: "C:\ProgramData\fkeabad\Autoit3.exe" C:\ProgramData\fkeabad\efghhgd.au3 MD5: C56B5F0201A3B3DE53E561FE76912BFD)
  - cmd.exe (PID: 7404 cmdline: cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - ADelRCP.exe (PID: 8100 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
    - SciTE.exe (PID: 7396 cmdline: C:\Program Files (x86)\autoit3\SciTE\SciTE.exe MD5: 91EE39F4A80F60A938095424EEF2C709)
      - msinfo32.exe (PID: 5644 cmdline: C:\Program Files (x86)\common files\microsoft shared\MSInfo\msinfo32.exe MD5: 29F917BF3DE95D7CE5B6B38CB7A895AB)
    - MyProg.exe (PID: 8056 cmdline: C:\Program Files (x86)\autoit3\Examples\Helpfile\Extras\MyProg.exe MD5: FE48113F3A78F980634E8CDACABF5091)
- ADelRCP.exe (PID: 8016 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8024 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8032 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8040 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8048 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8064 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8072 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- ADelRCP.exe (PID: 8080 cmdline: C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe MD5: 408995FA63F7BA3E059C8E32356B86C4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Autoit3.exe PID: 4108	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: cmd.exe PID: 4696	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: Autoit3.exe PID: 7204	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: cmd.exe PID: 7404	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: SciTE.exe PID: 7396	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

Networking

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

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

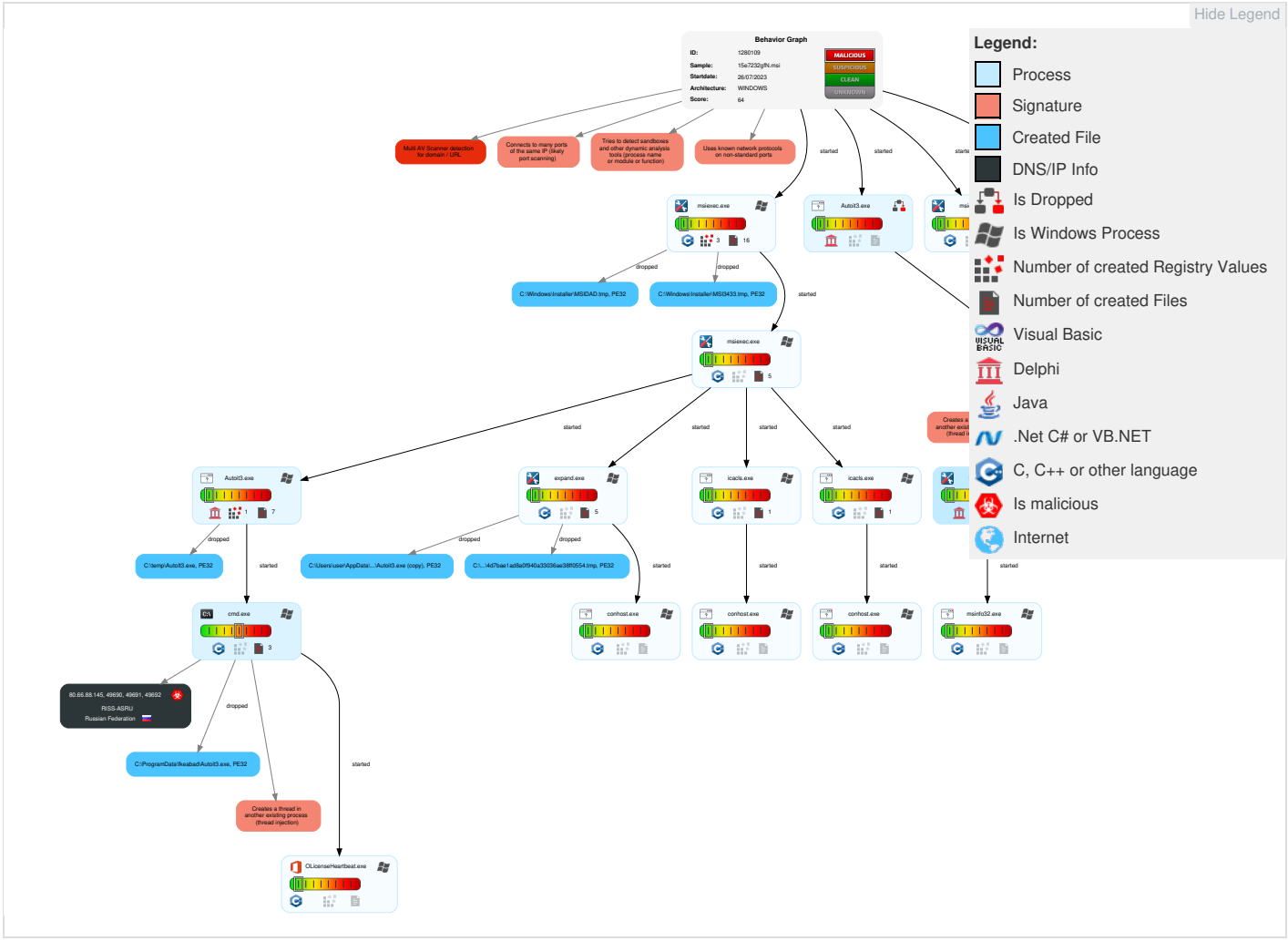
HIPS / PFW / Operating System Protection Evasion

Creates a thread in another existing process (thread injection)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 Input Capture	1 1 Peripheral Device Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	2 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Services File Permissions Weakness	2 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Services File Permissions Weakness	1 DLL Side-Loading	NTDS	4 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Masquerading	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 2 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Services File Permissions Weakness	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

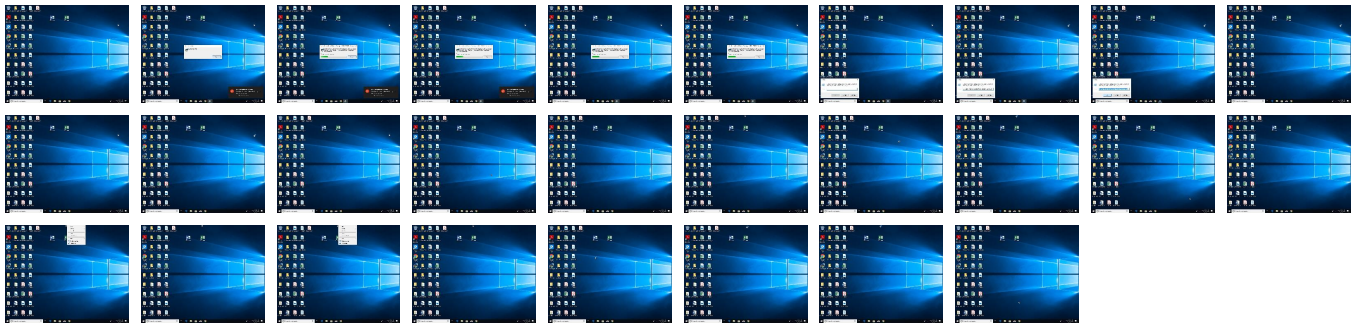
Behavior Graph



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
15e7232gfN.msi	2%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\fkeabad\Autoit3.exe	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\224f4e28a4d4462680bba17a3145169ddpx.tmp\4d7bae1ad8a0f940a33036ae38ff0554.tmp	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe (copy)	3%	ReversingLabs		
C:\Windows\Installer\MSI3433.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIDAD.tmp	0%	ReversingLabs		
C:\temp\AutoIt3.exe	3%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://80.66.88.145:9999d	0%	Avira URL Cloud	safe	
http://80.66.88.145&	0%	Avira URL Cloud	safe	
http://80.66.88.145:7891/	6%	Virustotal		Browse
http://80.66.88.145:9999n	0%	Avira URL Cloud	safe	
http://80.66.88.145:9999l	0%	Avira URL Cloud	safe	
http://80.66.88.145	7%	Virustotal		Browse
http://80.66.88.145	0%	Avira URL Cloud	safe	
http://80.66.88.	0%	Avira URL Cloud	safe	
http://80.66.88.145:7891/	0%	Avira URL Cloud	safe	
http://80.66.88.145:9999pT$	0%	Avira URL Cloud	safe	
http://80.66.88.145:9999	0%	Avira URL Cloud	safe	
http://80.66.88.145:7891	0%	Avira URL Cloud	safe	
http://80.66.88.145:9999x	0%	Avira URL Cloud	safe	
http://80.66.88.145:9999hd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://80.66.88.145:7891/	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

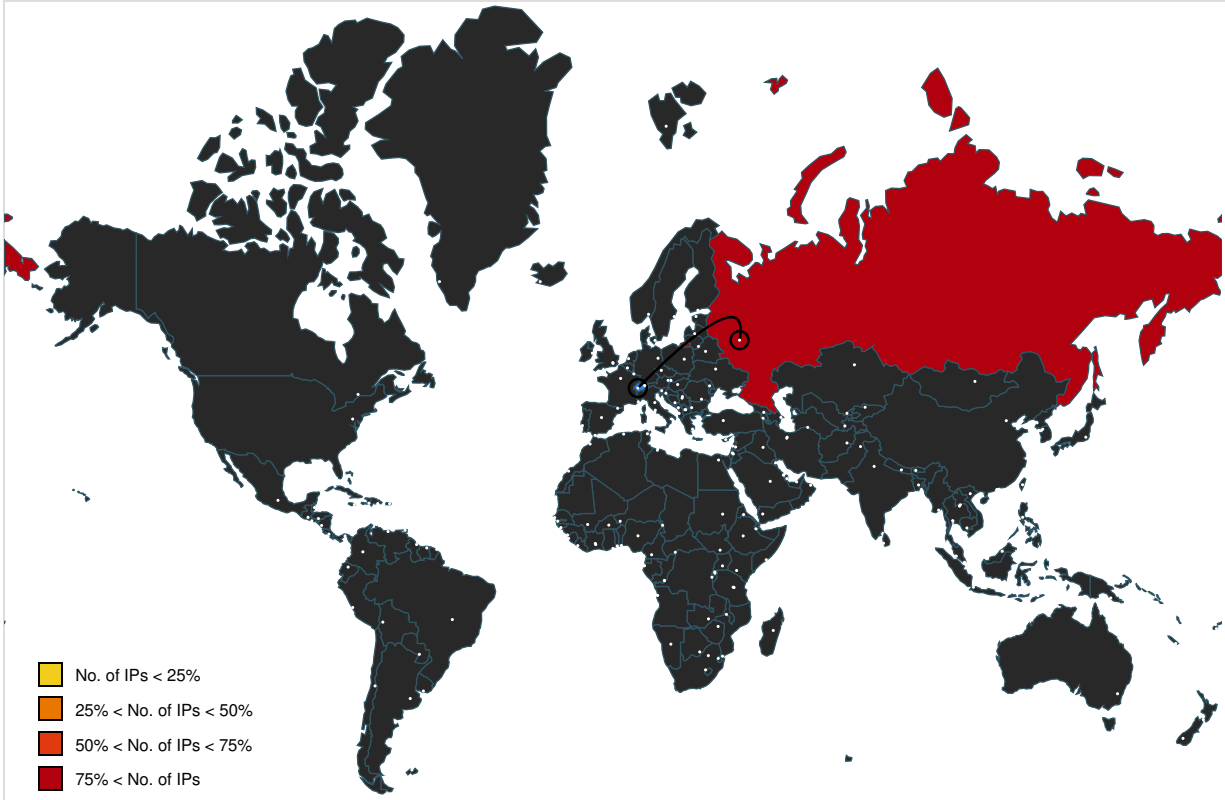
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://80.66.88.145	cmd.exe, 0000000E.00000002.708417301.000000000517B000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 0000000E.00000002.707423919.0000000004F93000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000002.820052302.0000000008EE4000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000002.818520760.00000000082A0000.00000004.00001000.00020000.00000000.sdmp	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	Autoit3.exe, 00000008.00000003.562124824.0000000004693000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 00000008.00000000.557064508.0000000000A49000.00000002.00000001.01000000.00000007.sdmp, Autoit3.exe, 00000008.00000003.561146540.0000000004693000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 00000008.00000002.567488146.0000000004482000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000002.614481086.0000000005043000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000003.565892356.00000000057C3000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000003.568468689.0000000005BC7000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 0000000D.00000003.592030670.0000000005033000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 0000000D.00000000.589433696.0000000000F59000.00000002.00000001.01000000.00000000B.sdmp, Autoit3.exe, 0000000D.00000002.598455223.0000000004C03000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000000E.00000003.596629594.0000000005703000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 0000000E.00000002.707423919.0000000004F93000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000003.685906923.0000000008C13000.00000004.00001000.00020000.00000000.sdmp	false		high
http://80.66.88.145:9999d	SciTE.exe, 00000018.00000002.818520760.00000000082A0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.145&	Autoit3.exe, 00000008.00000002.567488146.0000000004482000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.145:9999	SciTE.exe, 00000018.00000002.820052302.000000008EE4000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000002.818520760.00000000082A0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.145:9999n	SciTE.exe, 00000018.00000002.818520760.00000000082A0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.145:9999l	cmd.exe, 00000009.00000002.616883860.0000000005FBC000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000002.614739543.000000000522B000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000002.818520760.00000000082A0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.	SciTE.exe, 00000018.00000002.820052302.000000008EE4000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.autoitscript.com/autoit3/	Autoit3.exe, 00000008.00000003.562124824.0000000004693000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 00000008.00000003.561146540.0000000004693000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 00000008.00000002.567488146.0000000004482000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000002.614481086.0000000005043000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000003.565892356.00000000057C3000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 00000009.00000003.568468689.0000000005BC7000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 0000000D.00000003.592030670.0000000005033000.00000004.00001000.00020000.00000000.sdmp, Autoit3.exe, 0000000D.00000002.598455223.0000000004C03000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 0000000E.00000003.596629594.0000000005703000.00000004.00001000.00020000.00000000.sdmp, cmd.exe, 0000000E.00000002.707423919.0000000004F93000.00000004.00001000.00020000.00000000.sdmp, SciTE.exe, 00000018.00000003.685906923.0000000008C13000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://80.66.88.145:7891	cmd.exe, 00000009.00000002.614739543.000000000522B000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.145:9999pT$	cmd.exe, 00000009.00000002.614290853.0000000004E60000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.145:9999x	cmd.exe, 00000009.00000002.616707929.0000000005B00000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://80.66.88.145:9999hd	SciTE.exe, 00000018.00000002.820052302.000000008EE4000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.66.88.145	unknown	Russian Federation		20803	RISS-ASRU	true

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1280109
Start date and time:	2023-07-26 13:59:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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
Sample file name:	15e7232gfN.msi
Original Sample Name:	6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70.msi
Detection:	MAL
Classification:	mal64.troj.evad.winMSI@51/27@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 97.3%) • Quality average: 78.9% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:01:03	API Interceptor	4x Sleep call for process: Autoit3.exe modified
14:01:06	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\aafaecg.lnk
14:01:08	API Interceptor	13x Sleep call for process: cmd.exe modified
14:02:03	API Interceptor	35x Sleep call for process: SciTE.exe modified
14:02:27	API Interceptor	1x Sleep call for process: MyProg.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\fkeabad\Autoit3.exe

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z....."....@.....@...@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\ProgramData\fkeabad\efghhgd.au3

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	784356
Entropy (8bit):	6.500990461253042
Encrypted:	false
SSDEEP:	12288:6byAIRMKMJZCL+TWHZMxdHQgCUCAH2zxMSTaiTDBCphXUgn+DRVnNsPlU0R/Nexe:OgLQQgogvXUnsPlU0ZNMlpZ
MD5:	ED1131E98DAD331D3FEB1C38B2C6BA51
SHA1:	BB3F4522D7D0D3F4D5B9917019242AE5496F6F16
SHA-256:	B68861CDFC100021261A1F3067324628A31E85BA7EE3857FBD496D4AEFB2E68D
SHA-512:	06BD7E2E7F72A2E572435773DDC20E22D25168DF923ADAFD8535367A9D6722AFA04EFA3D5A21737BDB5146F8B29F23DFEF6B281E007AFF10A98696A998D2469
Malicious:	false
Preview:	EktKhsozeEMDfgFPspSgUITVIwePrSdclBFnEMpeDODwqjBTbROJhkbDHevTyQGdqDwFyyUCpvRCEbYaZUNLgppVeVpWwhmPZmmlcipfAhFvyXwZaLSKhOTf HGhoEgdIiEkfgvgrQldGJJrrJlNHdwsEqEBnwvpSFPeNhIwaeDLLWqdtxoWcrTQbvMmixcbpVlylekPIEMiqdrYjDizYZGNtFNntqyrKAqDaBplqSWmaYIsEehnWIfhTRS RnIBmCGKqjFcfTPYbwFBwkYhPazHvaxYqiovLdrfsrcxtOHqNkeGwvVlqOovwAdHqzbNJoDxaBjvtiVgVZzZzsAGPqtBBuHcIIQCaXbOssSKVwAgfxdeLVhJSnIYzYybsf IjDFplgYCanmHLmnfMjObTSLIEBOibFnGwfDMgOYpVfBPXsgXjUtmTSrxitGJjQDUztUEXxAKSGyUzMOebPVIxEnKrhEolGAJVcvUnboZkwDeJSWaoRsYzBi GIvbECSEqHPMARcvUiFBUwtrssSwLeRnbEnBBjBojbllhBOHPTIriuiMObKHpvulqujarQThNQSZrsjjGtEoePqXczimSQMoxrgDGLqIEglXwzXMTDPSgzgLapWowOjiZA zHqUAwqyMOGlxCGnjTiccUEwMBUVIgcVgUGTnZHMSTVZMtDgdtpEPoNljCTaSWqwtnhXHXroWxhuFAVNnJdWoLFwSJWVjTeSZXNYTToMoxZgCMzHavnBCdoj qbsLKLmQjwKxwuukhGXdMrKgZtaxWkZadvrEjQiVHxCBWgKhPwskdhBysLQwWZeQCzSQiYWDyaicnMrwthsKgAARKQxRnsWWiGLWPBehosNuxTvpaOVRlnOl frcJPkZanZEyZsQTdbTIOkmvPgSbrOdEdidFJyQjizWlsQTSrSuEKwgOOLQRiXHLBAoUlgaUgQcdiQEgaSzzUnyRWVoZhiusWPQyVeoasvdayNTDzuKvkuNujOAqsrMfgN

C:\ProgramData\fkeabad\kadfedf\afhbfhd

Process:	C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe
File Type:	data
Category:	dropped
Size (bytes):	129
Entropy (8bit):	6.439332390998306
Encrypted:	false
SSDEEP:	3:diG/sNsJ5jJEcApcAPmC2tWGBikSFIiBWCNmpn:T/sN+JEcA+1thBikSFJWGmp
MD5:	EFE32663E95C34B9E5DFD8EA4CE9E337
SHA1:	C4AFC04189F77CB661A3ADBFCB7B77989CBB0AFE
SHA-256:	8B5BFA938B0DEA6D29384BE513A887FA4EC94FD08CF68520E3C51E4B17A7CB31

SHA-512:	AF1C463891E0FBCA195DF8B39B5DC63CFE04FECABD1C569DD36E894AB52CB7CFD481D3901F93670D7CC74F5CCA9A37E37A41DF06DB13ABBC6F88F35BC7FA B74B
Malicious:	false
Preview:	qaLiJpqL4.....h.o]....a.....S.[........<f..'.....6I...8.C4a.....r.....h..s.f.....GW.v..o..... G.0T.8P.....S...

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, many, 1669773 bytes, 2 files, at 0x2c +A "Autoit3.exe" +A "UGtZgHHT.au3", ID 56955, number 1, 51 datablocks, 0 compression
Category:	dropped
Size (bytes):	1669773
Entropy (8bit):	7.004183948977661
Encrypted:	false
SSDEEP:	24576:eT9FsEsyt8l+E+s1tB7parWM0+AL5QgZQvUXtAqlU0ZyMRpF:k9FBJZEH1X1arF0vN/nXr
MD5:	E7C3B16ED93B760546AE6756B12644DA
SHA1:	99B3B1AF70B45B4B815A814F61F9B6E509CD3BB6
SHA-256:	659733A584C52078AC6B568DFB34A089BEF2B3835A5EA737D32C1623A468B743
SHA-512:	B6EEAAEEB1F7C8335076075BC8033D5D4744544F3937EEADDCBEF5F7BA257A64C20A47F8388C1E8F10C5821DA8ABE0683BE8FD60C3E1A9AEA25E4A705E2F8 B41
Malicious:	false
Preview:	MSCF.....z.....,.....{...e...3.....VB. .Autoit3.exe.....VB. .UGtZgHHT.au3.t/.Y....MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R.+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z... .....".....@.....@...@.....@.....@.....|.....P.....p...q...;..... [..@.....text..... ....`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\224f4e28a4d4462680bba17a3145169ddpx.tmp \4d7bae1ad8a0f940a33036ae38ff0554.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....".....@.....@...@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\224f4e28a4d4462680bba17a3145169ddpx.tmp \e004f9e1ae4f094daad741c0c79b7d17.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	775656
Entropy (8bit):	6.502577735066428
Encrypted:	false
SSDEEP:	12288:pbyAIRMKMJZCL+TWHZMxdHQgCUCAH2zxMSTaiTDBCphXUgn+DRVnNsPlU0R/NexP:RgLQQgogvXUnsPlU0ZNMIpc
MD5:	1B524D03B27B94906C1A87B207E08179
SHA1:	8FBAD6275708A69B764992B05126E053134FB9E9
SHA-256:	1AF981D9C5128B3657CDB5506D61563E0D1908B957E5DD6842059D6D3CFDC622
SHA-512:	1E0F2AEA5DAA40B6CB7DF61BA86E0956356AB7B7ECFC9E2934BC85EEC8D42D3AEB32858DD0EAD24E82EF261A4120F6374263B7AF9256EB79A294D51273CC4 F6E
Malicious:	false

Preview:	gljkbYNCNUfursQiNLDiefLJGttBjSzXQUkRysaJsXXdirQcwaLmzgXoNPNONKwsODeXMxFNCHdwkqrpLPKUWGVWZcMGbyYOHbJqwCXdIZwPTNCjYkYRchZQ ekJghDciYmDkJRShuIlyIzENsAKsbaYreZfsvOzjeocrnvFRJXTQjOCSUfQlJCfmvQOvlqiphrdcymZlTRXibmzduBSNrVizOIFwYNOMhQshljhIFSmVYVuNBygNXinpnk OBldfzWknVZZNNQnOvQIlcPMFCbmdjlMHRBEPqigVkPqVvSWNfwWRQzpaYlZGVtjMBEezMpudtrKjNqrEtOohMPoLuBhzBOhSOhKNbHWnpNDClhITJVRWlHU RJTqHpOPVOcYintOlrTlAzIlvyYEYwTDilBcBQecgMkQimvhkudUWAwPojfUXreOlXUKaVMsQTECkCDvyVnIlywfGqHADINlknXFyIcTFvnTKBzbOOZBjUVqWtVEwUjKae oWlxMulHtTYrEHiyrsfyxPOSrIfnxioUZMTTPrJPicsPiaqWaWKnazcoxJhOAKrIRbPSDMiiUneEqcIHmVhzQdLIRXalhCjSdGEBLrbdZPsgZPrFTSeMxOdkijhiXcCzFp SrlwTQTpsDWyiqrjEQRCBQizWUrMSdTIHXwczMfQiTMtIPEmlNjWLItLzEnmFWnAsYOUjoPTNSZdElnXWdgBqDJOOOvDJsAuMRVmzecAIzWqMusmWtXXwTL tuPfqsrLKEqrYepQbSMXdSPAYGsUpGGhKKvxOjlesJcFJqNJsrAXGYNHBhAdYCWaVRiGToHKlbbViGuJuTBWdLjBJUNmITdNgKyammmCuUzdwwljXarfgkyR KCoOlooltYDenkWAORfCLiqYPcsOndLipbFMLzWHJdyzXPOqBJOxvpQkLcOuGxAWHBFQwjAHbkeZfiyIOzQChoZztSlCdbczrBypPfAlqsfBhakdfGPkMFhMvcTZhYffyL

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53MyyzI0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....".....@.....@...@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3 (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	775656
Entropy (8bit):	6.502577735066428
Encrypted:	false
SSDEEP:	12288:pbyAIRMKMJZCL+TWHZMxdHQgCUCAH2zxMSTaiTDBCphXUgn+DRVnNsPIU0R/NexP:RgLQQgogvXUnsPIU0ZNMIpc
MD5:	1B524D03B27B94906C1A87B207E08179
SHA1:	8FBAD6275708A69B764992B05126E053134FB9E9
SHA-256:	1AF981D9C5128B3657CDB5506D61563E0D1908B957E5DD6842059D6D3CFDC622
SHA-512:	1E0F2AEA5DAA40B6CB7DF61BA86E0956356AB7B7ECFC9E2934BC85EEC8D42D3AEB32858DD0EAD24E82EF261A4120F6374263B7AF9256EB79A294D51273CC4 F6E
Malicious:	false
Preview:	gljkbYNCNUfursQiNLDiefLJGttBjSzXQUkRysaJsXXdirQcwaLmzgXoNPNONKwsODeXMxFNCHdwkqrpLPKUWGVWZcMGbyYOHbJqwCXdIZwPTNCjYkYRchZQ ekJghDciYmDkJRShuIlyIzENsAKsbaYreZfsvOzjeocrnvFRJXTQjOCSUfQlJCfmvQOvlqiphrdcymZlTRXibmzduBSNrVizOIFwYNOMhQshljhIFSmVYVuNBygNXinpnk OBldfzWknVZZNNQnOvQIlcPMFCbmdjlMHRBEPqigVkPqVvSWNfwWRQzpaYlZGVtjMBEezMpudtrKjNqrEtOohMPoLuBhzBOhSOhKNbHWnpNDClhITJVRWlHU RJTqHpOPVOcYintOlrTlAzIlvyYEYwTDilBcBQecgMkQimvhkudUWAwPojfUXreOlXUKaVMsQTECkCDvyVnIlywfGqHADINlknXFyIcTFvnTKBzbOOZBjUVqWtVEwUjKae oWlxMulHtTYrEHiyrsfyxPOSrIfnxioUZMTTPrJPicsPiaqWaWKnazcoxJhOAKrIRbPSDMiiUneEqcIHmVhzQdLIRXalhCjSdGEBLrbdZPsgZPrFTSeMxOdkijhiXcCzFp SrlwTQTpsDWyiqrjEQRCBQizWUrMSdTIHXwczMfQiTMtIPEmlNjWLItLzEnmFWnAsYOUjoPTNSZdElnXWdgBqDJOOOvDJsAuMRVmzecAIzWqMusmWtXXwTL tuPfqsrLKEqrYepQbSMXdSPAYGsUpGGhKKvxOjlesJcFJqNJsrAXGYNHBhAdYCWaVRiGToHKlbbViGuJuTBWdLjBJUNmITdNgKyammmCuUzdwwljXarfgkyR KCoOlooltYDenkWAORfCLiqYPcsOndLipbFMLzWHJdyzXPOqBJOxvpQkLcOuGxAWHBFQwjAHbkeZfiyIOzQChoZztSlCdbczrBypPfAlqsfBhakdfGPkMFhMvcTZhYffyL

C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1512
Entropy (8bit):	3.6912619977233305
Encrypted:	false
SSDEEP:	24:Fmw5dX8DW8XjkLvl0HSEwg7fdrF39wJ9wEy29w8Ut8Jh:nYqjEDfhF39wJ9wEl9wltSh
MD5:	406526B602B613C1EC5672387B911B74
SHA1:	FBF498C6CA5781ECAFD94E44CC9168F07E5E96BC
SHA-256:	F7082EACF5238976BB9C51F2B86AC92201B6AB693584B5E90A94859A477D226A
SHA-512:	4EE4998A66FAF86BC43FEB263ABACF25E876E20CD9A07E937F0E089F4893D011B7BD0740DC4AEA2FDB0B71BA62961615E868FF62C98AD921D7B3E9C3CC4FB C7A

Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=.{.2.C.B.A.8.8.3.F.-.5.1.A.6.-.3.D.7.D.-.D.B.B.9.-.0.5.2.7.D.3.9.4.3.3.C.B.}...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.n.e.v.e.r...B.a.s.e.N.a.m.e.=.A.u.t.o.i.t.3...e.x.e...C.a.b.H.a.s.h.=.6.5.9.7.3.3.a.5.8.4.c.5.2.0.7.8.a.c.6.b.5.6.8.d.f.b.3.4.a.0.8.9.b.e.f.2.b.3.8.3.5.a.5.e.a.7.3.7.d.3.2.c.1.6.2.3.a.4.6.8.b.7.4.3...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=.U.G.t.Z.g.H.H.T...a.u.3. ...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.F.I.L.E.S.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.b.b.b.4.0.9.b.2.-.5.2.b.d.-.4.c.e.9.-.a.b.7.7.-.0.8.6.8.4.7.a.6.4.4.a.4.\...F.i.l.e.s.D.i.r.=.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.b.b.b.4.0.9.b.2.-.5.2.b.d.-.4.c.e.9.-.a.b.7.7.-.0.8.6.8.4.7.a.6.4.4.a.4.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\aafaecg.lnk

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Archive, ctime=Wed Jul 26 11:01:05 2023, mtime=Wed Jul 26 11:02:00 2023, atime=Wed Jul 26 11:01:05 2023, length=893608, window=hide
Category:	dropped
Size (bytes):	891
Entropy (8bit):	4.50280361390797
Encrypted:	false
SSDEEP:	12:8DeLKdcqCzee/NuAkj/BajAWbQbPAVjbPAoubPA1UiKDkmeukmeMBm:8C7fcA+5mAikPA9PA/PA1UJeeeMBm
MD5:	12A296AA09D7196EB34454D70B750991
SHA1:	13DD5F81CBBDD558B2BA94FF4F7A342BABF8F136
SHA-256:	CBFB56EC3F8A746F70B421486F68DD183291185C708CA06CD8D07090BECA0050
SHA-512:	EE6A91FD4AB5470EAED9AF5FEEFB9A95EE1D4237076CCC64C21D8E0B0F82734CBE1514FCE72582048B20F945CD9A9DB2416292B5BD0632BDFB9B57B0A962FF42
Malicious:	false
Preview:	L.....F.... ...C.....S.....G....P.O. .:i.....+00.../C:\.....`.1.....V"`..PROGRA~3..H.....L..V"`....F.....=...P.r.o.g.r.a.m.D.a.t.a.....V.1....V#`..fkeabad.@.....V"`.V(`....<.....N.f.k.e.a.b.a.d.....b.2.....V#` .Autoit3.exe.H.....V#`.V#`....x.....\G~.A.u.t.o.i.t.3...e.x.e.....Q.....-.....P.....'yV'.....C:\ProgramData\fkeabad\Autoit3.exe..:.....\.....\.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m.D.a.t.a.\.f.k.e.a.b.a.d.\.A.u.t.o.i.t.3...e.x.e...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.f.k.e.a.b.a.d.\."C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.f.k.e.a.b.a.d.\.e.f.g.h.h.g.d...a.u.3.`.....X.....468325.....!a..%.H.VZAj....,r.h.....!a..%.H.VZAj....,r.h.....E.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Windows\Installer\5f09c5.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {609A83EA-2275-4DEA-858D-BAEFF01E16D0}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2
Category:	dropped
Size (bytes):	1921024
Entropy (8bit):	6.966994454036273
Encrypted:	false
SSDEEP:	24576:ftncpVGP4I9FsEsyt8l+E+s1tB7parWM0+AL5QgZQvUXtAqlU0ZyMRp:epUP59FBJZEH1X1arF0vN/nX
MD5:	247A8CC39384E93D258360A11381000F
SHA1:	23893F035F8564DFEA5030B9FDD54120D96072BB
SHA-256:	6E068B9DCD8DF03FD6456FAEB4293C036B91A130A18F86A945C8964A576C1C70
SHA-512:	336ECA9569C0072E92CE16743F47BA9D6BE06390A196F8E81654D6A42642FF5C99E423BFED00A8396BB0B037D5B54DF8C3BDE53757646E7E1A204F3BE271C99
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI3403.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	818
Entropy (8bit):	5.483919835925761
Encrypted:	false
SSDEEP:	12:EgSByEK+c8Ov/3khF1ETUYhl/3C8Ov/3khF1Eb8fNEHWot3jtnLx298A6nok9eW:aB9C8Ov/3khANhQ8Ov/3khAD2K0mh
MD5:	4F56271E25939DB53E061A846385F042
SHA1:	120015D53F237F56A5DFB77A1F6198CFC684ECC9
SHA-256:	47B0A4D7E04A361A15D7DC2D05F82F5FAE2030CC75B3B86F93CFC21FE7F4B13A
SHA-512:	404CF7E3610F9B04ADFF4F9C235B780099692A68379D97B484098E211B577B132B9E7E45F5A089EDA653235D7CA4A25AB6C1466C8CB61BCE303A701276820928
Malicious:	false

Preview:	...@IXOS.@.....@#p.V.@.....@.....@.....@.....@.....@.....@.....&.{229FD164-E132-4ADB-8998-1DB40BF25484}h.Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..15e7232gfN.msi.@.....@.....@.....@.....@.....&.{609A83EA-2275-4DEA-858D-BAEFF01E16D0}.....@.....@.....@.... .@.....@.....@.....@.....@....h.Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.]....&.{E DE10F6C-30F4-42CA-B5C7-ADB905E45BFC}^.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\{2CBA883F-51A6-3D7D-DBB9-0527D39433CB}\LogonUs er.@.....@.....@.....@.....@.....@.....@....

C:\Windows\Installer\MSI3433.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSIDAD.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\SourceHash{229FD164-E132-4ADB-8998-1DB40BF25484}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.163838104196163
Encrypted:	false
SSDEEP:	12:JSbX72FjjYAGiLIlHVRpZh/77777777777777777777777vDHFs5QgAit/l0i5:JJYQl5ttyiF
MD5:	F72F21050D099A517E88C0B9B95BD295
SHA1:	FB927683D4D37559DFE5FF69609B5538620180E2
SHA-256:	C5F264EB1A5BF5F5C0BE377CA6AEEE1D891B78A6A14623185C05425B6E2F25F6
SHA-512:	BE41F6A86A13013A291CD9ABAC362DED02039FEAE472982B6AE0930D592ECA16CD549BEEC7C28D3CB65BC6FBE2EA016B062DE56DCD936B62A3D9603351CC 35D3
Malicious:	false

Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5513830917935394
Encrypted:	false
SSDEEP:	48:R8PhYuRc06WXJ0nT5a5Kft/p51ddSromrXvddSB2FrMsUk4:shY13nThf9l0qUUk
MD5:	39D002620A197EA3B427C08D601946F3
SHA1:	14AC8566875EFD30752AD110761404EBF50EBEBE
SHA-256:	1C703D763A36E66B8DD0014B862B08F0334E2F66DEB2AB5906EB8EAC23421FA4
SHA-512:	E294C9F7FE77E87FAF5C3E77A7F222E3DD4218B7125B3F566DAC6C8DC07682BC5C696F2B07A77196333153B7FCA556104169DADA59AD788079CB9C242C7C4A2
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Logs\DPX\setupact.log	
Process:	C:\Windows\SysWOW64\expand.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	933929
Entropy (8bit):	4.386149343450665
Encrypted:	false
SSDEEP:	192:kKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcKqKcKnKcI:h
MD5:	32EE505C5647886928E3D11C54BBA7E4
SHA1:	FE772CBD72DDA16D080E59E10B50FD959E2F1E66
SHA-256:	A7AD713CC2A21F50E2B827BA4FCB58FEEE88920AFA94168186271887C685665E
SHA-512:	AB3FF4C69EDB64D2556B26E7546D6480F3067C2A7C16FAC02B590599927DD35EF7930E8B5690810E1FFDC1139A1896163AE91D81DBC17A584B4C75198F7D5B6
Malicious:	false
Preview:	.2019-06-27 00:56:09, Info DPX Started DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX CJob::Resume completed with status: 0x0..2019-06-27 00:56:09, Info DPX Ended DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Resume and Download Job..2019-06-27 00:56:09, Info DPX Started DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info DPX Ended DPX phase: Apply Deltas Provided In File..2019-06-27 00:56:09, Info

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	79122
Entropy (8bit):	5.282175982976613
Encrypted:	false
SSDEEP:	192:jmXs969ozNSkk3peTBYeHt0tfol9qsjl0urmwYyiLP:yXs9UogeWeH29qclhmwYyiz
MD5:	0C40CFAD0BD2539422CAA8F57D8193EA
SHA1:	DB665B3A82042D8CAD0C44B633C9C1D219AA1B14
SHA-256:	BF4A8A2D82A6517F468C4471B0B2394A23EFC2CAEC4C0207924D9B7C3147292B
SHA-512:	15B466CC7BF90D7A1CD8719930B878B13E960E300443846EC0B80D2EF0320E7E360B0CBE29BE06324CD293A6C524085A4C259619CE22C9F5C77CA8D4D6FCC00
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 03:22:38.143 [320]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.159 [320]: ngen returning 0x00000000..07/23/2020 03:22:38.222 [3748]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.237 [3748]: ngen returning 0x00000000..07/23/2020 03:22:38.284 [64]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.300 [64]:

C:\Windows\Temp\~DF0723A498380A03EB.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5513830917935394
Encrypted:	false
SSDEEP:	48:R8PhYuRc06WXJ0nT5a5Kft/p51ddSromrXvddSB2FrMsUk4:shY13nThf9l0qUUk
MD5:	39D002620A197EA3B427C08D601946F3
SHA1:	14AC8566875EFD30752AD110761404EBF50EBEBE
SHA-256:	1C703D763A36E66B8DD0014B862B08F0334E2F66DEB2AB5906EB8EAC23421FA4
SHA-512:	E294C9F7FE77E87FAF5C3E77A7F222E3DD4218B7125B3F566DAC6C8DC07682BC5C696F2B07A77196333153B7FCA556104169DADA59AD788079CB9C242C7C4A2
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF932E910C2B5A509D.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB46B19848F66B19D.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2421153914563245
Encrypted:	false
SSDEEP:	48:5zQuWNveFXJLT5Q5Kft/p51ddSromrXvddSB2FrMsUk4:BQMzTff9l0qUUk
MD5:	B1A8670826B5F77BC753BCADC495A828
SHA1:	98D51716C6EBE6688D045C74A540A048ECBFFC0A
SHA-256:	A11AF4BFF8668BD6C80241C2597A694CBD390AB752F6B37BEC7940D03EE6313A
SHA-512:	17BC3BE2FF878149E9B7416160269A9CA59C69425CE3A48C1B3AC6833C7D55871239E70725864666719 49EEDE8A5679CA1760ECB8099CF53FC38D2D28108441D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFB7831024D2CFB248.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07110935099595517

Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOcd5Qxq1yTTkgVky6lit/:2F0i8n0itFzDHFs5Qgzit/
MD5:	3903929F7674F66DDD40C1E48FE49788
SHA1:	6F61DA648B2F115CFFC54AB5B7D759621AF3C3B7
SHA-256:	D4930E8C3E3CCC91D00F852652EB2EDA8788F1810878386A06F48BA422EFDB66
SHA-512:	0A279D3708A5B942E4F7DEC5C9A921668798CAE13F015150C852F80D326F49019A6B54DD4C56F2AF8EF70A5647C405996AF93A708184B9B479E06DCDF13BF896
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB924194BEFC5CCB1.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.13751697623807846
Encrypted:	false
SSDEEP:	24:04D7sUMClNCwY+QJfAebfddipV72nddipVJV2BwGslrkg9SkuK52+kmKfKc5:04/sUwrfddSB2nddSromrX752JjfN5
MD5:	330881AB07C50808A453FA9D40A83756
SHA1:	E68EE2C966806A4C4E9E705653ED77B43053D68C
SHA-256:	61075C0EA7272B6F7C4C4237A4156886F4569170CBC662B8CBA05584745FC90E
SHA-512:	6D0F76A866468244A553055B597E2CCD8B1492F5E93CF9BE2B0C3810CE1DC01A6B7A41F783A327304270E83BA7AD49A6B473188A33B318E415938CE0085118EC
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFBA084C2D02A8EEAB.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\temp\AutoIt3.exe

Process:	C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....".....@.....@...@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\temp\efghhgd.au3	
Process:	C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	775656
Entropy (8bit):	6.502577735066428
Encrypted:	false
SSDEEP:	12288:pbyAIRMKMJZCL+TWHZMxdHQgCUCAH2zxMSTaiTDBCphXUgn+DRVnNsPlU0R/NexP:RgLQQgogvXUnsPlU0ZNMIpc
MD5:	1B524D03B27B94906C1A87B207E08179
SHA1:	8FBAD6275708A69B764992B05126E053134FB9E9
SHA-256:	1AF981D9C5128B3657CDB5506D61563E0D1908B957E5DD6842059D6D3CFDC622
SHA-512:	1E0F2AEA5DAA40B6CB7DF61BA86E0956356AB7B7ECFC9E2934BC85EEC8D42D3AEB32858DD0EAD24E82EF261A4120F6374263B7AF9256EB79A294D51273CC4 F6E
Malicious:	false
Preview:	gljkbYNCNUfursQiNLDiefLJGttBjSzXQUkRysaJsXXdirQcwaLmzgXoNPNONKwsODeXMxFNCHdwkqrpLPKUWGVWZcMGbyYOHbJqwCXdIZwPTNCjYkYRchZQ ekJghDciYmDkJRShuIlyIzENsAKsbaYreZfsvOzjeocrnvFRJXTQjOCSUfQlJCfmvQOvlqiphrdcymZITRXibmzduBSNrVizOIFwYNOMhQshljhIFSmVYVuNBygNXinpnk OBldfzWknVZZNNQnOvQIlcPMFCbmdjlMHRBEPqigVkPqVvSWNfwWRQzpaYIZGVtjMBEezMpudtrKjNqrEtOohMPoLuBhzBOhSOhKNbHWnpNDClhITJVRWlHU RJTqHpOPVOcYintOlrTlAzIlvyYEYwTDilBcBQecgMkQimvhkudUWAwPojfUXreOlXUKaVMsQTECkCDvyVnIlywfGqHADINlknXFyIcTFvnTKBzbOOZBjUVqWtVEwUjKae oWIxMulHtTYrEHiyrsfyxPOSrlfnxioUZMTTPrJPicsPiaqWaWKnazcoxJhOAKrlRbPSDMiiUneEqcIHmVhzQdLIRXalhCjSdGEBLrbdZPsgZPrFTSeMxOdkijhiXcCzFp SrlwTQTpsDWyiqrjEQRCBQizWUrMSdTIHXwczMfQiTMtIPEmlNjWLIItLzEnmFWnAsYOUjoPTNSZdElnXWdgBqDJOOOvDJsAuMRVmzecAIzWqMusmWtXXwTL tuPfqsrLKEqrYepQbSMXdSPAYGsUpGGhKKvxOjlesJcFJqNJsrAXGYNHBhAdYCWaVRiGToHKlbbViGuJuTBWdLjBJUNmITdNgKyammmCuUzdwwljXarfgkyR KCoOlooltYDenkWAORfCLiqYPcsOndLipbFMLzWHJdyzXPOqBJOxvpQkLcOuGxAWHBFQwjAHbkeZfiyIOzQChoZztSlCdbczrBypPfAlqsfBhakdfGPkMFhMvcTZhYffyL

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\expand.exe
File Type:	ASCII text, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	264
Entropy (8bit):	4.799289113892546
Encrypted:	false
SSDEEP:	6:zx3MmSLQHtBXVNsR+/HomwD0DIZJQiOC0n:zK/0HtBFNEqIBD0DYJQiI
MD5:	95817EBB90389A8FD4D35E30A512A8ED
SHA1:	DF6DF33A5BB54BC0640C449E226E7A6D4B2E08D1
SHA-256:	B8DFD73944D25D6E6067A5C684571A20E19FB796AFE200A51449AF60D6D0A751
SHA-512:	6786337517865661084B906DA28BE8915313DF5A14380066E9D30A3813E5FD9E0FBB9D9D559D408DCAA74E85E787FBEED8B69A7BC030064AB8F94816834D8A5E
Malicious:	false
Preview:	Microsoft (R) File Expansion Utility..Copyright (c) Microsoft Corporation. All rights reserved.....Adding files\Autoit3.exe to Extraction Queue..Adding files\UGtZgHHT.au3 to Extraction Queue....Expanding Files .....Expanding Files Complete .....2 files total...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {609A83EA-2275-4DEA-858D-BAEFF01E16D0}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating A pplication: MSI Wrapper (10.0.51.0), Security: 2
Entropy (8bit):	6.966994454036273
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	15e7232gfN.msi
File size:	1'921'024 bytes
MD5:	247a8cc39384e93d258360a11381000f
SHA1:	23893f035f8564dfea5030b9fdd54120d96072bb
SHA256:	6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70
SHA512:	336eca9569c0072e92ce16743f47ba9d6be06390a196f8e81654d6a42642ff5c99e423bfed00a8396bb0b037d5b54df8c3bde53757646e7e1a204f3be271c998
SSDEEP:	24576:ftncpVGP4I9FsEsyt8l+E+s1tB7parWM0+AL5QgZQvUXtAqlU0ZyMRp:epUP59FBJZEH1X1arF0vN/nX

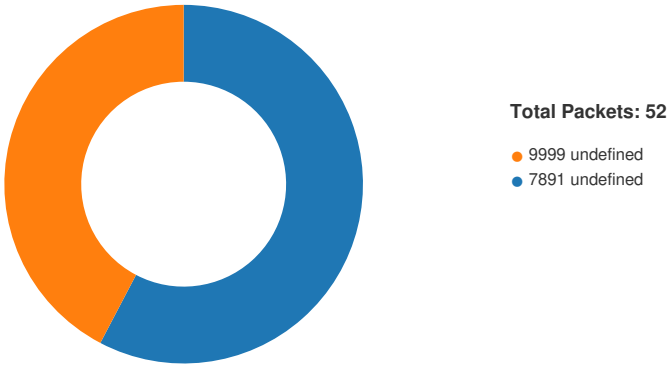
TLSH:	A895AE4273B7F022FE9BD132565EEE06317C6C643262E56F239C3869D9301B2663D62D
File Content Preview:	.....>.....

File Icon

Icon Hash:	2d2e3797b32b2b99

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2023 14:01:05.669145107 CEST	49690	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.681461096 CEST	49691	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.712990999 CEST	7891	49690	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.713164091 CEST	49690	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.713223934 CEST	49690	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.715008020 CEST	9999	49691	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.789221048 CEST	7891	49690	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.789556980 CEST	7891	49690	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.789592028 CEST	7891	49690	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.789676905 CEST	49690	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.789733887 CEST	49690	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.802953959 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.830910921 CEST	7891	49690	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.843775988 CEST	7891	49692	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.843946934 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.844060898 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.880832911 CEST	7891	49692	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.880882978 CEST	7891	49692	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.881006956 CEST	7891	49692	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:05.881062984 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.881115913 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.881158113 CEST	49692	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:05.914927959 CEST	7891	49692	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:06.219929934 CEST	49691	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:06.255738020 CEST	9999	49691	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:06.766566038 CEST	49691	9999	192.168.2.4	80.66.88.145

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2023 14:01:06.810133934 CEST	9999	49691	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:06.810844898 CEST	49693	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:06.849031925 CEST	9999	49693	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:07.360358000 CEST	49693	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:07.393773079 CEST	9999	49693	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:07.907313108 CEST	49693	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:07.940556049 CEST	9999	49693	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:08.058561087 CEST	49694	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:08.099719048 CEST	9999	49694	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:08.641751051 CEST	49694	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:08.681644917 CEST	9999	49694	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:09.235543013 CEST	49694	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:09.269253969 CEST	9999	49694	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:09.409147978 CEST	49695	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:09.443409920 CEST	9999	49695	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.048125029 CEST	49695	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.081598997 CEST	9999	49695	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.505003929 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.538868904 CEST	7891	49696	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.539031029 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.539072990 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.574842930 CEST	7891	49696	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.576016903 CEST	7891	49696	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.576062918 CEST	7891	49696	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:10.576136112 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.576136112 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.735654116 CEST	49695	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:10.778984070 CEST	9999	49695	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.321501017 CEST	49696	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.348306894 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.355397940 CEST	7891	49696	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.386725903 CEST	7891	49697	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.386933088 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.422662973 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.430847883 CEST	49698	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.465109110 CEST	9999	49698	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.466541052 CEST	7891	49697	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.466737986 CEST	7891	49697	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.466835022 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.466973066 CEST	7891	49697	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:11.467170000 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.485348940 CEST	49697	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:11.518922091 CEST	7891	49697	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:12.048228025 CEST	49698	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:12.081741095 CEST	9999	49698	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:12.735822916 CEST	49698	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:12.769140005 CEST	9999	49698	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:12.877263069 CEST	49699	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:12.911011934 CEST	9999	49699	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:13.548459053 CEST	49699	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:13.584130049 CEST	9999	49699	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:14.124579906 CEST	49699	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:14.161727905 CEST	9999	49699	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:14.284281015 CEST	49700	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:14.322448969 CEST	9999	49700	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:14.829849958 CEST	49700	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:14.874561071 CEST	9999	49700	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.376637936 CEST	49700	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.416196108 CEST	9999	49700	80.66.88.145	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 26, 2023 14:01:15.526289940 CEST	49701	9999	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.554184914 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.559758902 CEST	9999	49701	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.589715004 CEST	7891	49702	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.589864969 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.589994907 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.624844074 CEST	7891	49702	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.624886990 CEST	7891	49702	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.625071049 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.625096083 CEST	7891	49702	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.625353098 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.636919975 CEST	49702	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.677680969 CEST	7891	49702	80.66.88.145	192.168.2.4
Jul 26, 2023 14:01:15.685345888 CEST	49703	7891	192.168.2.4	80.66.88.145
Jul 26, 2023 14:01:15.719986916 CEST	7891	49703	80.66.88.145	192.168.2.4

HTTP Request Dependency Graph

- 80.66.88.145:7891

Statistics

Behavior

- msiexec.exe
- msiexec.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- Autoit3.exe
- cmd.exe
- icacls.exe
- conhost.exe
- OLicenseHeartbeat.exe
- Autoit3.exe
- cmd.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- ADelRCP.exe
- SciTE.exe
- MyProg.exe
- msinfo32.exe

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: **7028**, Parent PID: **3528**

General

Target ID:	0
Start time:	14:00:54
Start date:	26/07/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\15e7232gfN.msi"
Imagebase:	0x7ff71c140000
File size:	66'048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **4764**, Parent PID: **576**

General

Target ID:	1
Start time:	14:00:54
Start date:	26/07/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff71c140000
File size:	66'048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	79028	94	30 37 2f 32 36 2f 32 30 32 33 20 31 34 3a 30 30 3a 35 35 2e 35 37 35 20 5b 34 37 36 34 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	07/26/2023 14:00:55.575 [4764]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FF87481BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FF87481BBC6	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **7100**, Parent PID: **4764**

General

Target ID:	3
Start time:	14:00:56
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding D8DD1A2B41DAA758FA08D3E85077DC6F
Imagebase:	0x1220000
File size:	59'904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: **7068**, Parent PID: **7100**

General

Target ID:	4
Start time:	14:00:57
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0x7ff7c72c0000
File size:	29'696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1236, Parent PID: 7068

General

Target ID:	5
Start time:	14:00:57
Start date:	26/07/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625'664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: expand.exe PID: 5484, Parent PID: 7100

General

Target ID:	6
Start time:	14:00:58
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0x1100000
File size:	52'736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6052, Parent PID: 5484

General

Target ID:	7
Start time:	14:00:58
Start date:	26/07/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625'664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Autoit3.exe PID: **4108**, Parent PID: **7100**

General

Target ID:	8
Start time:	14:00:59
Start date:	26/07/2023
Path:	C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe" UGtZgHHT.au3
Imagebase:	0x980000
File size:	893'608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3F1BCAA	CreateDirectoryA
c:\temp\efghhgd.au3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3F1BEB4	CreateFileA
c:\temp\AutoIt3.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3F1BEB4	CreateFileA
C:\ProgramData\fkeabad\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3F1BCAA	CreateDirectoryA
C:\ProgramData\fkeabad\kadfedf\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3F1BCAA	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\cfffbcb\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3F1BCAA	CreateDirectoryA
C:\ProgramData\fkeabad\kadfedf\afhbfhd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3F1BEB4	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\temp\efghhgd.au3	0	775656	67 6c 6a 6b 62 59 4e 43 4e 55 66 75 72 73 51 69 4e 4c 44 69 65 66 4c 4a 47 74 74 42 6a 53 7a 58 51 55 6b 52 79 73 61 4a 73 58 58 64 69 72 51 63 77 61 4c 6d 7a 67 58 6f 4e 50 4e 4f 4e 4b 77 73 4f 44 65 58 4d 78 46 4e 43 48 64 77 6b 71 72 70 4c 50 4b 55 57 47 56 57 5a 63 4d 47 62 79 59 4f 48 62 4a 71 77 43 58 64 49 5a 77 50 54 4e 43 6a 59 6b 59 52 63 68 5a 51 65 6b 4a 67 68 44 63 69 59 6d 44 6b 4a 52 53 68 75 49 6c 79 49 7a 45 4e 73 41 4b 73 62 61 59 72 65 5a 66 73 76 4f 7a 6a 65 6f 63 72 6e 76 46 52 4a 58 54 51 6a 4f 43 53 55 66 51 6c 4a 43 66 6d 76 51 4f 76 6c 71 69 70 68 72 64 63 79 6d 5a 6c 54 52 58 69 62 6d 7a 64 75 42 53 4e 72 56 69 7a 4f 49 46 77 59 4e 4f 4d 68 51 73 68 6c 6a 68 49 46 53 6d 56 59 56 75 4e 42 79 67 4e 58 69 6e 70 6e 6b 4f 42 6c 64 66	gljkbYNCNUfursQiNLDief LJGttBjS zXQUkRysaJsXXdirQcw aLmzgXoNPNO NKwsODeXMxFNCHdwk qrpLPKUWGVWZc MGbyYOHbJqwCXdIZwP TNCjYkYRchZQ ekJghDciYmDkJRShuIlyI zENsAKsba YreZfsvOzjeocrnvFRJXT QjOCSUfQl JCfmvQOvlqiphrdcymZlT RXibmzduB SNrVizOIFwYNOMhQshlj hIFSmVYVuN BygNXinpnkOBldf	success or wait	1	3F1C910	WriteFile
C:\temp\AutoIt3.exe	0	893608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 16 73 44 fd 52 12 2a fd 52 12 2a fd 52 12 2a fd 14 43 fd fd 50 12 2a fd 32 fd fd 53 12 2a fd 5f 40 fd fd 61 12 2a fd 5f 40 fd fd fd 12 2a fd 5f 40 fd fd 67 12 2a fd 5b 6a fd fd 5b 12 2a fd 5b 6a fd fd 77 12 2a fd 52 12 2b fd 72 10 2a fd fd fd fd 02 12 2a fd fd fd fd 53 12 2a fd 5f 40 fd fd 53 12 2a fd 52 12 fd fd 50 12 2a fd fd fd fd 53 12 2a fd 52 69 63 68 52 12 2a	MZ@!L!This program cannot be run in DOS mode.$sDR*R*R*CP*S*_ @a*_@*_@g*[j[* [jw*R+r**S*_@S*R P*S*RichR*	success or wait	1	3F1C910	WriteFile
C:\ProgramData\fkeabad\kadfedf \afhbfhd	0	129	71 61 4c 69 4a 70 71 4c 34 fd fd fd fd fd 68 15 6f 5d 2e fd fd fd 61 fd 7f 10 18 fd 53 fd 5b fd fd 07 fd fd fd fd fd 3c 66 fd 1c 27 0c fd 0a 1e fd 36 49 fd fd 0c 38 fd 43 34 61 fd 9c fd 10 fd fd 72 12 fd fd fd fd 68 fd fd 73 2e 66 08 fd 16 fd 1f fd 47 57 12 76 11 fd 6f fd fd 0c fd fd fd fd fd fd 7f fd 20 47 fd 30 54 fd 38 50 fd fd fd 02 fd 1d fd fd fd fd 53 fd 06 8f	qaLiJpqL4ho].aS[<f'6I8C 4arhs.fGWvo G0T8PS	success or wait	1	3F1C910	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	65536	success or wait	11	9B12FD	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	4096	success or wait	1	9B12FD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	512	success or wait	2	9B12FD	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	512	success or wait	1	9B12FD	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	112640	success or wait	1	9B12FD	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	775656	success or wait	1	36C30B7	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3F1C9A8	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe	unknown	893608	success or wait	1	3F1C9A8	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	775656	success or wait	1	3F1C9A8	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\UGtZgHHT.au3	unknown	775656	success or wait	1	3F1C9A8	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting	DontShowUI	dword	1	success or wait	1	3F15101	RegSetValueExA

Analysis Process: cmd.exe PID: **4696**, Parent PID: **4108**

General

Target ID:	9
Start time:	14:01:03
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe
Imagebase:	0xd90000
File size:	232'960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\fkeabad\Autoit3.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	45BEB4	CreateFileA
C:\ProgramData\fkeabad\efghhgd.au3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	45BEB4	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\fkeabad\kadfedf \afhbfhd	0	129	71 61 4c 69 4a 70 71 4c 34 fd fd fd fd fd 68 15 6f 5d 2e fd fd fd 61 fd 7f 10 18 fd 53 fd 5b fd fd 07 fd fd fd fd fd 3c 66 fd 1c 27 0c fd 0a 1e fd 36 49 fd fd 0c 38 fd 43 34 61 fd 9c fd 10 fd fd 72 12 fd fd fd fd 68 fd fd 73 2e 66 08 fd 16 fd 1f fd 47 57 12 76 11 fd 6f fd fd 0c fd fd fd fd fd fd 7f fd 20 47 fd 30 54 fd 38 50 fd fd fd 02 fd 1d fd fd fd fd 53 fd 06 8f	qaLiJpqL4ho].aS[<f'6I8C 4arhs.fGWvo G0T8PS	success or wait	1	45C910	WriteFile
C:\ProgramData\fkeabad\Autoit3.exe	0	893608	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 16 73 44 fd 52 12 2a fd 52 12 2a fd 52 12 2a fd 14 43 fd fd 50 12 2a fd 32 fd fd 53 12 2a fd 5f 40 fd fd 61 12 2a fd 5f 40 fd fd fd 12 2a fd 5f 40 fd fd 67 12 2a fd 5b 6a fd fd 5b 12 2a fd 5b 6a fd fd 77 12 2a fd 52 12 2b fd 72 10 2a fd fd fd fd 02 12 2a fd fd fd fd 53 12 2a fd 5f 40 fd fd 53 12 2a fd 52 12 fd fd 50 12 2a fd fd fd fd 53 12 2a fd 52 69 63 68 52 12 2a	MZ@!L!This program cannot be run in DOS mode.$sDR*R*R*CP*S*_ @a*_@*_@g*[j[* [jw*R+r**S*_@S*R P*S*RichR*	success or wait	1	45C910	WriteFile
C:\ProgramData\fkeabad\efghhgd.au3	0	784356	45 6b 74 4b 68 73 6f 7a 65 45 4d 44 66 67 46 50 73 70 53 67 55 49 54 56 49 77 65 50 72 53 64 63 6c 42 46 6e 45 4d 70 65 44 4f 44 77 71 6a 42 54 62 52 4f 4a 68 6b 62 44 48 65 76 54 79 51 47 64 71 44 77 46 79 79 55 43 70 76 52 43 45 62 59 61 5a 55 4e 4c 67 70 70 56 65 56 70 57 77 68 6d 50 5a 6d 6d 6c 63 69 70 66 41 68 46 76 79 58 77 5a 61 4c 53 4b 68 4f 54 66 48 47 68 6f 45 67 64 49 69 45 6b 66 67 76 67 72 51 6c 64 47 4a 4a 72 72 4a 49 4e 48 64 77 73 45 71 45 42 6e 77 76 70 53 46 50 65 4e 68 49 77 61 65 44 4c 4c 57 71 64 74 78 6f 57 63 72 54 51 62 76 4d 6d 69 78 63 62 70 56 6c 79 6c 65 6b 50 6c 45 4d 69 71 64 72 59 6a 44 69 7a 59 5a 47 4e 74 46 4e 6e 74 71 79 72 4b 41 71 44 61 42 70 6c 71 53 57 6d 61 59 49 73 45 65 68 6e 57 49 66 68 54 52 53 52 6e 49 42 6d	EktKhsozeEMDfgFPspSg UITVIwePrS dclBFnEMpeDODwqjBTb ROJhkbDHevT yQGdqDwFyyUCpvRCEb YaZUNLgppVeV pWwhmPZmmlcipfAhFvy XwZaLSKhOTf HGhoEgdIiEkfgvgrQldGJ JrrJINHdw sEqEBnwvpSFPeNhIwae DLLWqdtxoWc rTQbvMmixcbpVlylekPlE MiqdrYjDi zYZGNtFNntqyrKAqDaB plqSWmaYIsE ehnWIfhTRSRnIBm	success or wait	1	45C910	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	45C9A8	ReadFile
C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\files\Autoit3.exe	unknown	893608	success or wait	1	45C9A8	ReadFile
C:\ProgramData\fkeabad\kadfedf\afhbfhd	unknown	129	success or wait	1	45C9A8	ReadFile
C:\temp\efghhgd.au3	unknown	775656	success or wait	1	45C9A8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: **6980**, Parent PID: **7100**

General

Target ID:	10
Start time:	14:01:05
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-bbb409b2-52bd-4ce9-ab77-086847a644a4\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0x940000
File size:	29'696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4952**, Parent PID: **6980**

General

Target ID:	11
Start time:	14:01:05
Start date:	26/07/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625'664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: OLicenseHeartbeat.exe PID: **3132**, Parent PID: **5172**

General

Target ID:	12
Start time:	14:01:12
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\common files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe
Imagebase:	0xe20000
File size:	124'632 bytes
MD5 hash:	CFD37109A4E595C2957C5E0ACC198E8A
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: Autoit3.exe PID: **7204**, Parent PID: **3528**

General

Target ID:	13
Start time:	14:01:14
Start date:	26/07/2023
Path:	C:\ProgramData\fkeabad\Autoit3.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\fkeabad\Autoit3.exe" C:\ProgramData\fkeabad\efghhgd.au3
Imagebase:	0xe90000
File size:	893'608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 3%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\fkeabad\efghhgd.au3	unknown	65536	success or wait	11	EC12FD	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	4096	success or wait	1	EC12FD	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	512	success or wait	2	EC12FD	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	512	success or wait	1	EC12FD	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	112640	success or wait	1	EC12FD	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	3CB30B7	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	489C9A8	ReadFile
C:\ProgramData\fkeabad\Autoit3.exe	unknown	893608	success or wait	1	489C9A8	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	489C9A8	ReadFile
C:\ProgramData\fkeabad\kadfedf\afhbfhd	unknown	129	success or wait	1	489C9A8	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	489C9A8	ReadFile

Analysis Process: cmd.exe PID: **7404**, Parent PID: **7204**

General

Target ID:	14
Start time:	14:01:17
Start date:	26/07/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe
Imagebase:	0xd90000
File size:	232'960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	45C9A8	ReadFile
C:\ProgramData\fkeabad\Autoit3.exe	unknown	893608	success or wait	1	45C9A8	ReadFile
C:\ProgramData\fkeabad\kadfedf\afhbfhd	unknown	129	success or wait	1	45C9A8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	45C9A8	ReadFile

Analysis Process: ADelRCP.exe PID: **8016**, Parent PID: **5172**

General	
Target ID:	15
Start time:	14:01:26
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8024**, Parent PID: **5172**

General	
Target ID:	16
Start time:	14:01:26
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8032**, Parent PID: **5172**

General	
Target ID:	17
Start time:	14:01:26
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8040**, Parent PID: **2940**

General

Target ID:	18
Start time:	14:01:27
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8048**, Parent PID: **4172**

General	
Target ID:	19
Start time:	14:01:27
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8064**, Parent PID: **3936**

General	
Target ID:	20
Start time:	14:01:28
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8072**, Parent PID: **3936**

General	
Target ID:	21
Start time:	14:01:28
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes

MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8080**, Parent PID: **3936**

General	
Target ID:	22
Start time:	14:01:28
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ADelRCP.exe PID: **8100**, Parent PID: **7404**

General	
Target ID:	23
Start time:	14:01:28
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\adobe\Acrobat Reader DC\Reader\ADelRCP.exe
Imagebase:	0x980000
File size:	138'800 bytes
MD5 hash:	408995FA63F7BA3E059C8E32356B86C4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SciTE.exe PID: **7396**, Parent PID: **2940**

General	
Target ID:	24
Start time:	14:01:45
Start date:	26/07/2023
Path:	C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\autoit3\SciTE\SciTE.exe
Imagebase:	0x400000
File size:	1'256'960 bytes
MD5 hash:	91EE39F4A80F60A938095424EEF2C709
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	1046C9A8	ReadFile
C:\ProgramData\fkeabad\Autoit3.exe	unknown	893608	success or wait	1	1046C9A8	ReadFile
C:\ProgramData\fkeabad\kadfedf\afhbfhd	unknown	129	success or wait	1	1046C9A8	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	1046C9A8	ReadFile

Analysis Process: MyProg.exe PID: **8056**, Parent PID: **7404**

General

Target ID:	25
Start time:	14:02:10
Start date:	26/07/2023
Path:	C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\autoit3\Examples\Helpfile\Extras\MyProg.exe
Imagebase:	0x1000000
File size:	2'560 bytes
MD5 hash:	FE48113F3A78F980634E8CDACABF5091
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	104EC9A8	ReadFile
C:\ProgramData\fkeabad\Autoit3.exe	unknown	893608	success or wait	1	104EC9A8	ReadFile
C:\ProgramData\fkeabad\kadfedf\afhbfhd	unknown	129	success or wait	1	104EC9A8	ReadFile
C:\ProgramData\fkeabad\efghhgd.au3	unknown	784356	success or wait	1	104EC9A8	ReadFile

Analysis Process: msinfo32.exe PID: **5644**, Parent PID: **2932**

General

Target ID:	26
Start time:	14:02:49
Start date:	26/07/2023
Path:	C:\Program Files (x86)\Common Files\microsoft shared\MSInfo\msinfo32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\common files\microsoft shared\MSInfo\msinfo32.exe
Imagebase:	0xed0000
File size:	337'920 bytes
MD5 hash:	29F917BF3DE95D7CE5B6B38CB7A895AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly