MALICIOUS

Classifications: Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Alphaware.exe**
ID	#4443708
MD5	d6cf5f8289eac27c551334578e6e4d9f
SHA1	25f581c79b08f85ffe729bfec35fdc1ba6ef0add
SHA256	3a2b0d7aa2a94d6d537838a2a18fa25890c2df97c7708e895f7c566f7a65ab76
File Size	1078.00 KB
Report Created	2023-05-18 11:17 (UTC)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 56 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #2) svchost.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) svchost.exe renames multiple user files.			
5/5	User Data Modification	Modifies Windows automatic backups	2	-
	• (Process #2) svchost.exe deletes Windows volume shadow copies. • (Process #3) cmd.exe deletes Windows volume shadow copies.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 455 files by appending the extension ".alphaware".			
3/5	System Modification	Disables a Windows system tool	1	-
	• (Process #2) svchost.exe disables startup repair by executing ""C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #2) svchost.exe possibly drops ransom note files (creates 52 instances of the file "readme.txt" in different locations).			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) svchost.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #7) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #2) svchost.exe sets the desktop wallpaper to the file "C:\Users\kEecfMwgj\AppData\Local\Temp\300wkaa5g.jpg".			
1/5	Privilege Escalation	Enables process privilege	3	-
	• (Process #1) alphaware.exe enables process privilege "SeDebugPrivilege". • (Process #2) svchost.exe enables process privilege "SeDebugPrivilege". • (Process #7) wmic.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) alphaware.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) svchost.exe tries to gather information about application "Mozilla Firefox" by file.			
1/5	Discovery	Enumerates running processes	2	-
	• (Process #1) alphaware.exe enumerates running processes. • (Process #2) svchost.exe enumerates running processes.			
1/5	Persistence	Installs system startup script or application	2	-

Score	Category	Operation	Count	Classification

- (Process #2) svchost.exe adds "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.url" to Windows startup folder.
- (Process #2) svchost.exe adds "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini.Alphaware" to Windows startup folder.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Changes folder appearance	34	-

- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Desktop".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Links".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Contacts".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Documents".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Downloads".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Pictures".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Music".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\OneDrive".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Saved Games".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Favorites".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Favorites\Links".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Searches".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\Videos".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Libraries".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\SendTo".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Documents".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Pictures".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Pictures\Sample Pictures".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Music".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Music\Sample Music".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Videos".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Videos\Sample Videos".
- (Process #2) svchost.exe changes the appearance of folder "C:\Users\Public\Desktop".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	3	-

- (Process #2) svchost.exe starts (process #3) cmd.exe with a hidden window.
- (Process #2) svchost.exe starts (process #11) cmd.exe with a hidden window.
- (Process #2) svchost.exe starts (process #14) cmd.exe with a hidden window.

Mitre ATT&CK Matrix

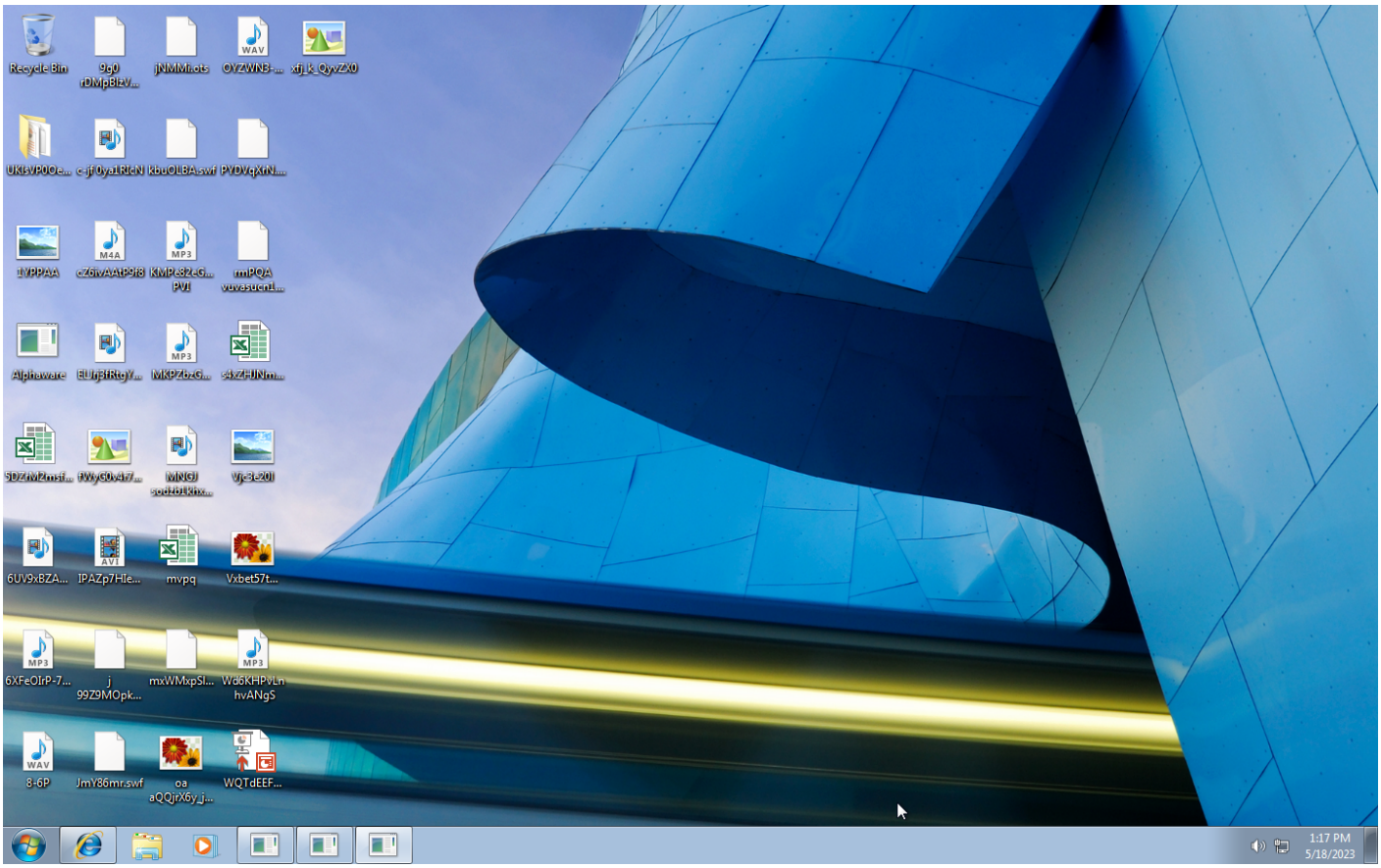
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1036 Masquerading	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1490 Inhibit System Recovery
				#T1143 Hidden Window		#T1057 Process Discovery		#T1005 Data from Local System			#T1491 Defacement
											#T1486 Data Encrypted for Impact

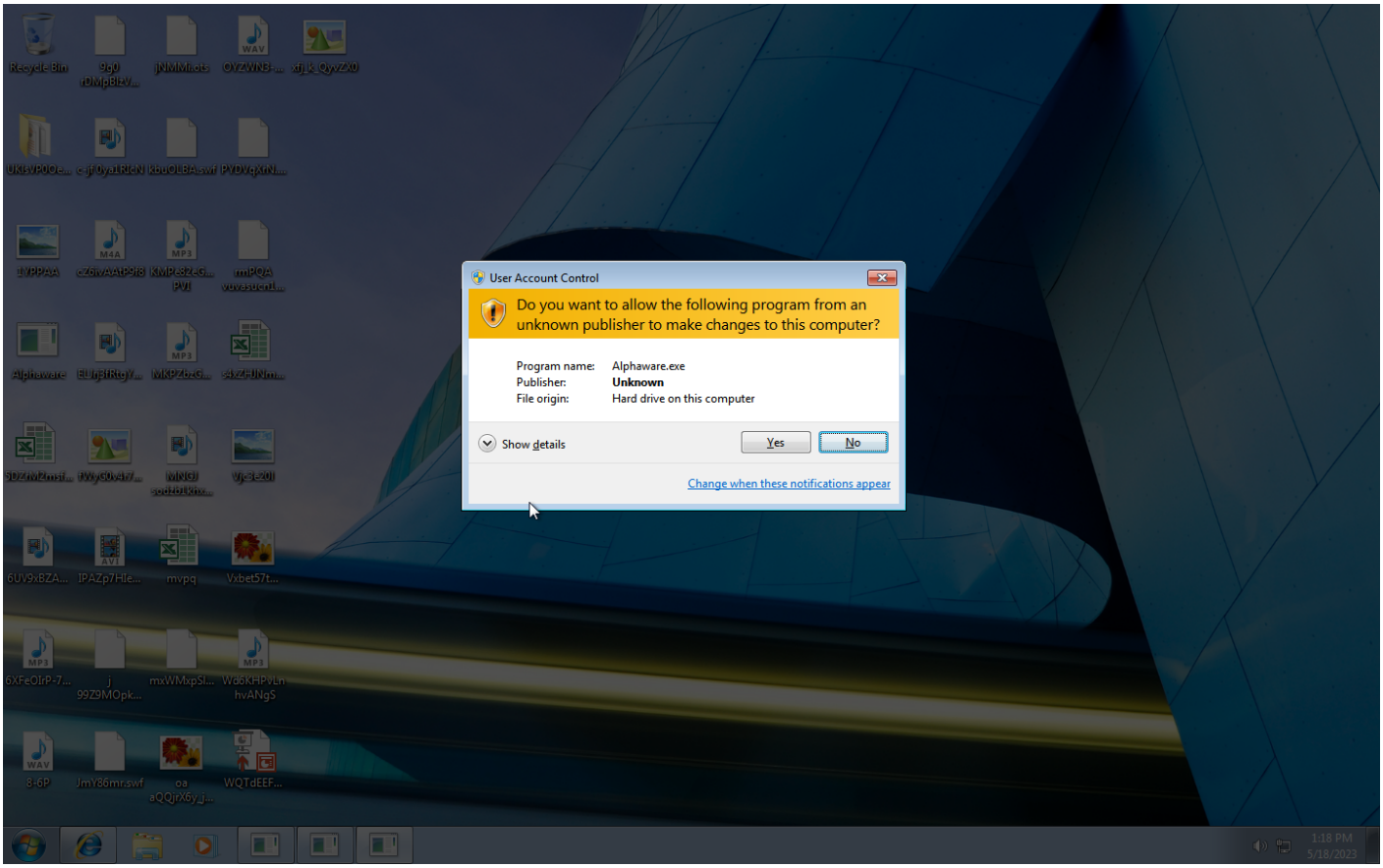
Sample Information

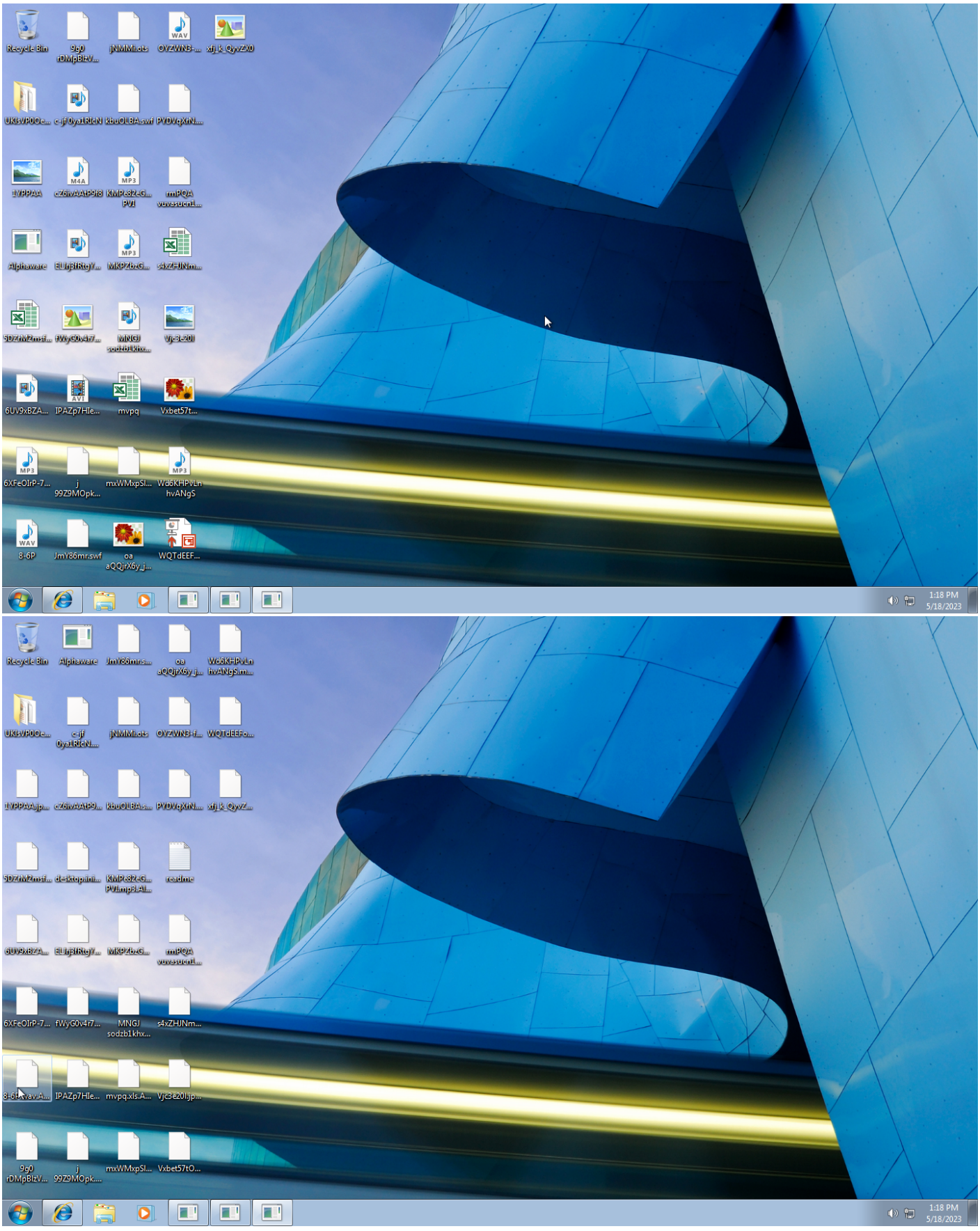
ID	#4443708
MD5	d6cf5f8289eac27c551334578e6e4d9f
SHA1	25f581c79b08f85ffe729bfec35fdc1ba6ef0add
SHA256	3a2b0d7aa2a94d6d537838a2a18fa25890c2df97c7708e895f7c566f7a65ab76
SSDeep	24576:CDmzI+4jJk5xYsx+1itfzYpjJU1P2UjStlezy:COIfaxLx+EEC2UVz
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	Alphaware.exe
File Size	1078.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-05-18 11:17 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	15
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✔
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: Alphaware.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

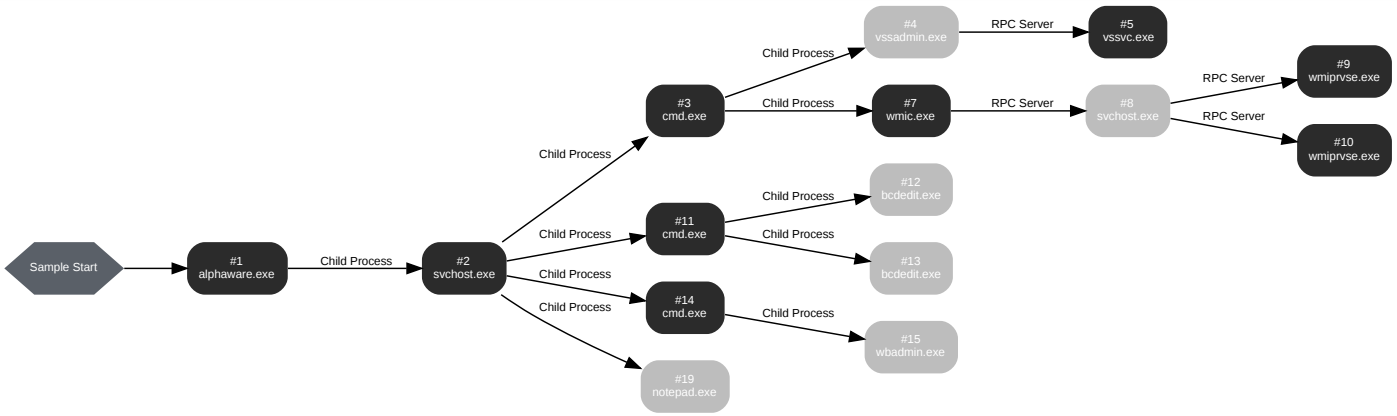
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: alphaware.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\alphaware.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\Alphaware.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 37116, Reason: Analysis Target
Unmonitor End Time	End Time: 59688, Reason: Terminated
Monitor duration	22.57s
Return Code	1
PID	3748
Parent PID	1932
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\Alphaware.exe	1078.00 KB	3a2b0d7aa2a94d6d537838a2a18fa25890c2df97c7708e895f7c566f7a65ab76	✖

Host Behavior

Type	Count
Registry	1
Module	1693
Environment	1
User	2
System	2
Process	94
File	2

Process #2: svchost.exe

ID	2
File Name	c:\users\keecfmwgj\appdata\roaming\svchost.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\svchost.exe"
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 57842, Reason: Child Process
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	219.29s
Return Code	Unknown
PID	3800
Parent PID	3748
Bitness	64 Bit

Dropped Files (421)

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\appdata\roaming\vcnvmrhf2u7xxjbaxrmb.pps.alphaware	70.66 KB	647d424bedc754a542ff702c0942983c7770fa53362fb738bd1042984bdb110d	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\4_p930hvcz_.lnk.alphaware	4.80 KB	5a4efb030996c150529030c7a10e1690fea0d6c2539048c0a60e84a86e36f130	✖
c:\users\keecfmwgj\desktop\1yppaa.jpg.alphaware	3.05 KB	ad2a49dd606aa339ca4b319d8a80b1db75ac2d28c651f082610e25f6c97b51b8	✖
C:\Users\kEecfMwgj\Documents\UgJB0bK8M6Fbzeqf.xlsx.Alphaware	52.66 KB	e71adbded09bb9f2e3e8f0c7b9affa3f51e7fe80eb1909fc2b65c241a4419853	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\y-0.lnk.alphaware	3.20 KB	2a9b3dacb01d464da3a7e4f99616955b2f99e8a1889dd61fa441200ddb8e9b52	✖
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\az80w8eavf6qldtcvji\r5baui uaurz 0kbpe.jpg.alphaware	32.97 KB	313de9e8e30738cb15c371b05a23ef7cd38a64a49f1e239eaae4f215f416bb47	✖
c:\users\keecfmwgj\appdata\roaming\n_rln0z3nrhzqdxjjzi.rtf.alphaware	14.11 KB	377db872cc28a0df07b74f5fc0bb4a0c94b70226ea066c4df1d4a0e7382b2547	✖
C:\Users\kEecfMwgj\Pictures\CGtmsH0_nmfPfsQOHtip\dFW79KlkBOtau4aDuO.jpg.Alphaware	35.32 KB	931d1667557f0bd9359a3609e9a2642e02a6d1b4188ab9dbf662ad3e42b366cd	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\iso690nmerical.xsl.alphaware	283.51 KB	4a0583e3b0ba5b60eb6b5c3de8402cf2ed92ce8f0fd9b209dcb7301e9cb617cd	✖
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\e1l_xrq6amcgtt.bmp.alphaware	73.61 KB	7b9865aa930ed83fcba80a30ec990f584e4840d0ac08295051ebeabf21e53684	✖
c:\users\keecfmwgj\appdata\roaming\im_qpwmgce7suron0abx.m4a.alphaware	84.99 KB	ad66744aa3633a14d2935cc338d6714763541707 78e22b7a2982b429ad9fcffe	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\6jCAQWe-_9EEl7aEUjN.lnk.Alphaware	1.41 KB	173bd505975005b2ec2170ab50c998622bc452f0ee09df9864bd0961739243d4	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\zR1JJINH15QPRebоG.lnk.Alphaware	8.61 KB	087ae75e0a159a72275d09cf544e386d1e6590da85f791c3aa295c6cbc0c043d	✖
c:\users\keecfmwgj\appdata\roaming\s8zdflucr_z28spu.swf.alphaware	55.78 KB	c5b3841d7aca576f0816a28fa54d39b0e61e1553fcc4c8537d40e60259086dd6	✖
C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\SjIEHWNzBPbEPK.ppt.Alphaware	119.76 KB	668cc94eb04575d906ec58194389f97d9eb5f3fffb731643433ab33eeb8be6a0	✖
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\readme.txt	1.15 KB	1f07fbece71d67c140a10aa9993f1d5bba5250f21b7cfafcc39e4ea60689223c	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\y- 0\beaeacczBwDfQo39\k3 HQLaJEyY.odp.Alphaware	109.86 KB	60ab82ccd03da740aef46884a83af55ff6a51a149d82c1ee06601bef8b60764f	✖
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\bC7JKZ.swf.Alphaware	115.41 KB	6e8e90934f9d13fe3028eba01d2c6651b02ebaf182dcb991893afcda991f7e7b	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\egl9rx1kxsqwh.mkv.lnk.alphaware	1.47 KB	7a9caacc4c976f2b317ec7589f209c1cf22b9b645cc6045bb69872a1e9e243c5	✖
c:\users\public\videos\sample videos\wildlife.wmv.alphaware	10240.00 KB	88224add061e5303e3776f409ec980ccdd0f13a56f72768a7b036a5011a60589	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vo9mo3eeu2 slpqjwfm.lnk.alphaware	5.30 KB	206c87ba6f0fdb1c2ad3eecf95d99af73ac4762a6f62b7768467407cfea182ae	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\h8wehqdt-nllywl7w3.lnk.alphaware	5.30 KB	5310fb2e5c77a90243ef2c5d8c43b2e8d2bc140e5a5ea64c79ea4d11015b9c07	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vmoqizt54.lnk.alphaware	8.01 KB	70bd7d4a2dcb825aa8bcf0ad2a353c9be79676a02e434190ab91a3c1c956674a	✖
c:\users\keecfmwgj\appdata\roaming\bnr8t.csv.alphaware	68.74 KB	014da00ff1825e399bac0e5f12f172b98af0577a15cfc89e024585ef500ed2af	✖
c:\users\keecfmwgj\desktop\cz6ivaatp9f8.m4a.alphaware	83.68 KB	1332129f0c4cb2e754a05843eda9390a336d128b4cc3d38adc34b8204a1baad9	✖
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\MADiRK5BENdO7pHH.flv.Alphaware	4.78 KB	ed92bbba46d682a29678f2baa60667cf2b16828caa597037ab06c2d2d31db339	✖
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\pOajqkURwLncz.wav.Alphaware	130.61 KB	2d25226ca002e584ab1b0d10b7dd311f6d646da5f95c88fe4a39fb4939abf526	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent_aoxubo1xfzs.lnk.alphaware	3.49 KB	4c8fa0396fd2a61e07bc2813a2c2e2e2eb22089a2fef40b0957c61bb8852ddf0	✖
c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\jc7ce.wav.alphaware	77.09 KB	deeefaba22ffd6bf20007e1cb993c49ddd6ac0f25d8bcb4cb8107466c85cdb7d	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\w0y6k3cxjraf-y2ue6.lnk.alphaware	3.38 KB	883389249f9db96cb607065a08ad0edb3adfc430e3534cf93b03604d8d8b246c	✖
c:\users\keecfmwgj\desktop\wqtdeefonuz7kxbdbx.pps.alphaware	20.05 KB	c29e95222f1f7b69c4a49c510f4e9e18b808556caac61e7703ebbdb02fcddbae	✖
c:\users\keecfmwgj\appdata\roaming\egl9rx1kxsqwh.mkv.alphaware	41.24 KB	1964528466328e1f4a269d6868f2189118d227d2a2ae77eb0fd10314f5b77ce8	✖
c:\users\keecfmwgj\documents\d_cm4s7fp.pptx.alphaware	40.49 KB	82aebf50d58b108d2cc2d316671e0bea8aad7d07b93f1c3a66cb3e2f79e2bc2a	✖
c:\users\keecfmwgj\appdata\roaming\nbyvlogs.m4a.alphaware	128.55 KB	74020efa349c1f6fc36e7341874bb6d3442cc5113100018aa3751e88593a3f29	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\nqr9nqmjn0 i.lnk.alphaware	6.34 KB	d1ef917db973ca1597d744e94d8f0ae35a7527cf10231dbf559412630313937d	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\eusz.lnk.alphaware	6.18 KB	deedee1a4c21146b82c3747bfc1147e63003f65a8221122ab44f6c6e0e7136ea	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\e4w8io-jmf.lnk.alphaware	4.68 KB	27e59fa0f2f5b8e750198cf15921267d930b26a2dadade7ad244f5b7ffe37254	✖
c:\users\keecfmwgj\pictures\sd_mf\96isf-4zdjysw7lw.png.alphaware	12.91 KB	87452060df99e73d3b29c5d6746c362eb7dbcd27198c9f474e460d5bd85d29a0	✖
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\JlGdXo.wav.Alphaware	119.93 KB	5d8b8bbdd997b313b5c953d6e5926cde314913f860c205768de4609f7f5af38c	✖
c:\users\keecfmwgj\videos\zdm5mb5uma.avi.alphaware	84.22 KB	7781c693865e7d9a548cbedd790cebfb7eabb9de186616b918d76ba78075566b	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\chicago.xsl.alphaware	386.95 KB	a98112f44d6dc1a1a2692b89c6a8f030407fc1120ffa539da3732a195d0b6ea0	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\bleMKBNSsvf5WRB.lnk.Alphaware	3.30 KB	140b0484da5f7937a9be1fe923ec2c1d134adc98b7391887a64300fb6b8900362	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\v8u50bnoh.lnk.alphaware	6.49 KB	7657d3b36626d1f25a9b10f020aa5e7c3a2863e1cd3478d5628c68d4c0854561	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl.Alphaware	383.70 KB	925f8cf001c8b395912cfbd3a4a15752636a4f114508c172ce37a3040d3019b1	✖
C:\Users\kEecfMwgj\Desktop\j 99Z9MOpk.pdf.Alphaware	86.16 KB	4b7cb1d030155aa2776fb7ecac443b0ffaa2ea145982127a6319350ea9de0275	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RBnxFLdoe6j5FMDq.lnk.Alphaware	3.30 KB	7293fef9c6a5654fe059791b1dfcb399a4da07bf79c99a81533e5914db95e5f9	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\MKqMrJd2GayW Iyftd.ots.lnk.Alphaware	3.51 KB	01e8f85a450cb53b54fa1035f74b303913fd9806495248f1fdde069b1cb1ac99	✖
C:\Users\kEecfMwgj\Desktop\desktop.ini.Alphaware	584 bytes	b11d6fbdbd5e1594b46d24c8e16d7d0b09478bcf8c90cbf613c41a00a650d619	✖
c:\users\keecfmwgj\appdata\roaming\z2r-dghdhevsmryotz.mp3.alphaware	106.70 KB	7a4f65b27831e3636dfc22966ff1468bca0097a40c332d89520f9ad9d3fc3c44	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\ozdqhhdycahwn.lnk.alphaware	3.49 KB	6a0833ab6a5d3205cf31df709ebc65de77cebf9a95ebcdd4401b93ee26117165	✖
c:\users\keecfmwgj\pictures\q_m8xgrwlwvpa_ok jpb.jpg.alphaware	94.28 KB	84e587044e798fd3d6b401b23a568d89d5be4c7d4bb874f13baa6cf149bb4563	✖
C:\Users\kEecfMwgj\Desktop\c-jf 0ya1RIcN.mp4.Alphaware	47.95 KB	081de4eaf8fe463b0b6f39224690fb73c1e9e5fb996333640d25dcaa2af1a18f	✖
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF Jl4_p930HVcZ_\c4x.flv.Alphaware	112.28 KB	99d430a38a82ad70c686c4273d85bac48d5918b942f4969e56265a705cf16a78	✖
c:\users\keecfmwgj\pictures\desktop.ini.alphaware	884 bytes	701414085c3180dd5e1513ed8a5e196be6abf2d1c7e565db9cf11f923668ee9d	✖
C:\Users\kEecfMwgj\Music\JtwiWA.m4a.Alphaware	23.80 KB	f04aecab34f432b855a6bb815f8688692b1be169b549af2336663276841e5322	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\dFW79KlkBOtau4aDuO.lnk.Alphaware	5.30 KB	b446e67d96853bfb56189698130157393b2d538eefebc8da56305f0ad97329d8	✖
C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQIR\eUSZ\awU7DFoRrK67OUHE2Uat.mp4.Alphaware	128.53 KB	f8bc15b261895fe111366d04df687c6ff8d5c4b3b726ee9641c8e32cc01c8401	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Cookies\keecfmwgj@login.microsoftonline[2].txt.Alphaware	756 bytes	91c2ade52e5c75e713a8d85dee590ce61563a39b5346feae931b1e9346c1db82	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\roaming.lnk.alphaware	1.18 KB	ac2dd5075ba5a47d6e9bd1d60469d45ed244bc90f407a7706fa7bc1c1a6155b9	✖
C:\Users\kEecfMwgj\Contacts\desktop.ini.Alphaware	756 bytes	c538c278ef89ca7befb259bb22e8ace75474a3253723504463023487 67f92010	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\bffgcaoao_f0b_.swf.lnk.alphaware	4.93 KB	78d5dafdeea54a2bae733365873a2212d6d04379fe6284a79f2a61c9ed3a3579	✖
C:\Users\kEecfMwgj\Music\5jdQ8S\t3tMVJXbAaJh1K.mp3.Alphaware	51.26 KB	e2411e9ce863c7b4d347408e994bd5e2b905d21350db863d6a13133211eaf1ff	✖
C:\Users\kEecfMwgj\Desktop\8-6P.wav.Alphaware	132.45 KB	54bb466e7a682006b523c0e39f54355f55d51fd6473a0f4281bf421ea0381bf2	✖
c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\onrpsaekvylzpjqzcm2l.mkv.alphaware	2.07 KB	b1a87382f1870b618aba80572827bd4bc22384163896b45301ffac77ebd141bd	✖
C:\Users\kEecfMwgj\Music\5jdQ8S\hX1YQpkZK 4fEglyKr.mp3.Alphaware	133.47 KB	52b121d159493b1614379294dae7d6e0788be7d71db5a5355ccbad849825f609	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\tvhtwfsg.flv.lnk.alphaware	4.95 KB	312fef44dad6a75a8bf7908b969fe9195f0569b3bc7e836c08d86521dc7bdc45	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\NQCf5ew.lnk.Alphaware	6.26 KB	853ec114bb1050fb0950e428e0ef78c47673ccb40720a1708b36fdde69906e9f	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\4a87c_8npb.lnk.alphaware	3.45 KB	fa3acd99f3a83d43efcb2df96455e08ef3befaee63a918aeb0b2f05421e9aad1	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\96isf-4zdjysw7lw.lnk.alphaware	4.93 KB	22b5c0695bf5fd512e62706caff6cc51d0191b72fe88b29b0804a66437890703	✖
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\1tTeAH3Idl9j.m4a.Alphaware	102.18 KB	b44c9ef9bf219eacfb5f515ec071c383fc461382646c8e0e239aaf0088b06dd8	✖
c:\users\keecfmwgj\documents\o4vmeo_pmk30fk6.xlsx.alphaware	13.95 KB	a5ac8e5a2200ab118f0db0e52611ae22560314021d4fc9d2585b635066f2d3c4	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\TKqjZN.flv.lnk.Alphaware	4.80 KB	34bcaf8fb00efe56b1c060041773689a44c190eccdda9adea2217550b6c5b510	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\shows desktop.lnk.alphaware	608 bytes	72c12a955553bd1afa872321069078c97e1c5c03b830b13e89b6921704056c57	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\oaaqqjrx6y_jtlap6.lnk.alphaware	992 bytes	8af6fb49b17eaaed2fa3f4cf431d04af654cefabbc6973793a9cbb7a999133c3	✖
c:\users\keecfmwgj\desktop\mngj sodzb1khxmh.mp4.alphaware	20.76 KB	04a2f40e8311cf9fc611869c82ea2ce3da5a391a62410d01a59f598b28dcdaa4	✖
c:\users\keecfmwgj\appdata\roaming\uk0_t4zjwac.wav.alphaware	41.24 KB	a89e973014b0dd3c75a4fd8b606310f39e8bb025b345a6008e7038d5522749d7	✖
C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\AZ80w8eAVF6qLdtcVJI\zR 1JJINH15QPReboG.png.Alphaware	76.99 KB	8d507f71fc8cf794b011e6f89540b5f259823f2dc4ed747ff8555c1c20944634	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl.Alphaware	434.59 KB	4db6323b8870408c05fb4a201ab98f2138550e930b8ff64cd6ea4fd383b4d669	✖
c:\users\keecfmwgj\music\5jdq8s\zmtegoau5-f.wav.alphaware	81.34 KB	1568ecdbdb04ae12543d3503e6ef1429c56711e7fa47b9fafc54cbd4ceefbd33	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\te-nh.flv.lnk.alphaware	1.41 KB	7680cd3936aa709277bbb3728202f45821e0b636267513d777aa4056235cecb7	✖
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\LIjGz_b-guf6pPz.wav.Alphaware	59.30 KB	1b6e4acceb33696e532f3d7cd556eb6d86d812ac176299e40ea52663addf77f	✖
C:\Users\kEecfMwgj\Desktop\mxWMxpSlb1Z2y3xfhO0.swf.Alphaware	76.26 KB	db3f053ea4f54eda35e451a115d6633cda8c38fa23dfa55512fdd7f18efd7a0f	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\9wzxgia1p9.lnk.alphaware	4.86 KB	080496dffcb29b25c5351a0373aa161589bd3fde67be5775093e742db4eac6e9	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\sD_Mf.lnk.Alphaware	3.20 KB	795908a0821f809e827b118e179138a434a3f17b0e56fc246de9f197c7080c3b	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\7cu9qgyf.lnk.alphaware	6.61 KB	cb2b7b7fc8ba818db9c65059f42b6c7a6546e068ebd77b7da4ce404e5357f7c5	✖
C:\Users\kEecfMwgj\AppData\Roaming\t2oMmxPi.flv.Alphaware	75.26 KB	b939cf5cd0e6c95ceb0bafb15a780e8050420bc31a675b60f00e5bb5d574e475	✖
c:\users\keecfmwgj\documents\y-0\beaeacczbwdfqo39\kxx8q7znvev6f aidqyx.xlsx.alphaware	64.43 KB	5644fcd3e7d867179b50f5f288cb63e519d0720195ce58674b886cc7ec87bcb8	✖
c:\users\keecfmwgj\appdata\roaming\2cvjqdl8abrh.rtf.alphaware	113.99 KB	6a642840f89898869706bf05374ae335ad25b67ee32dcc5a441c94c1c7bf7536	✖
c:\users\keecfmwgj\desktop\mkpzbzgpkyhpvsxosep3.mp3.alphaware	37.36 KB	9c1327904e184c164a59335ada2cdfe03e09ac1ce1f8b95de1ce145e917faece	✖
c:\users\keecfmwgj\links\recentplaces.lnk.alphaware	692 bytes	80055bedc01c07d618e091109c8f42ba78100d070d609d4f1524eceff97a67cf	✖
C:\Users\kEecfMwgj\Music\8wsZ\sRZM.m4a.Alphaware	100.74 KB	3fbdad8e1dc18b41fb570a3cb173ad32e8e7ede0c6bcd67d7ff6613bebe38697	✖
c:\users\keecfmwgj\videos\jvugc2sabzf j\0o6jwd.mp4.alphaware	60.36 KB	e402b6a03f67110975fd6df62a7e72c8e3a267951543719fcef7605d129210d0	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\1dc7CK 8O2M4jV0-v99j.doc.Alphaware	24.05 KB	1d212a645ef441eadf3d11529bed8eba5a963197ba9ec9d5f50a2c73663e1872	✖
C:\Users\kEecfMwgj\Videos\0vDMTR303fbv.avi.Alphaware	83.38 KB	badc04a6c6894af1b0b1a21ae9c7b72b947cbd6bf243d45d0ac92d5f26ae7003	✖
C:\Users\kEecfMwgj\Documents\y- 0\z8zS.rtf.Alphaware	96.41 KB	4b136cc0e370df5b17ad076b661dce603f0b61b00a6a2253a4df4ab240fff92f	✖
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\v8u50bnoh.bmp.alphaware	127.03 KB	dfabf4334aee5ed2a34fa05c3409bef441bb8176eb0bf5c05f1feb8f23b0333b	✖
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\mIvaw3l8e0fmzi-r4q.gif.alphaware	110.99 KB	c8251fb5b793785e6a1d6c592a17046c2ab012644c1975e7e79634b3175799ff	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\windows media player.lnk.alphaware	2.22 KB	0030e291131fe9e00e6658e67969401b1d63b1579a80d7b3c6e2fcbf933c93df	✖
C:\Users\kEecfMwgj\Searches\desktop.ini.Alphaware	904 bytes	81e080a6d94c56585dd6fad29bcb4a2f5e73b031a562cd57e3ba7ae0d42e24ee	✖
C:\Users\kEecfMwgj\Music\8wsZ\vGw-gK7bU.mp3.Alphaware	55.70 KB	9fdab2d83f2d480c414f22057e931ae5269a512f4ff3f97257eeb29859e2b725	✖
C:\Users\kEecfMwgj\Documents_aOXubo 1XFZS.docx.Alphaware	70.41 KB	671ead14985a314c03d5b144cb0d789e967081b9da840a86a28183bca7c9f68c	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\MADiRK5BENdO7pHH.flv.lnk.Alphaware	5.01 KB	96038f172abd4300b60a7eb2d8d024ef35010786e38ac144e12166700cc9ee22	✖
C:\Users\kEecfMwgj\AppData\Roaming\AcoFPdLUL2Wyq3ljkzb.jpg.Alphaware	108.61 KB	005895ea100e66ac1b752aec86e025267391b625df32c934bda8ce57bb098c09	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\7ord0oMkDdqdZwcFM7PM.mkv.lnk.Alphaware	1.51 KB	a2c0580d6653d755cd72893416ad3c5ad4f185829e2a29152abd7fb5964ac057	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\bJTM1.flv.lnk.Alphaware	6.55 KB	4a34518459689352942bc2d5824a79057f4a22577e9038c336451ad297152c69	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\hWvMFQJJJ.lnk.Alphaware	3.22 KB	c16813818833d936754c4c985250971a07b6e12483e158c14a24cbcb34826787	✖
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\eRiABnWG9I.m4a.Alphaware	83.74 KB	69a605a483b58d7ecc864dd6313dc3f1c679742d56bda131e44651d4bd7bd54e	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\300wkaa5g.jpg	969.78 KB	4e9ab5deb85ebedbe89416892dcdc6183edbdf4f9f5458a4c075f8cba8a4e276	✖
c:\users\keecfmwgj\appdata\roaming\wy-il 75unfs8bktr.wav.alphaware	114.30 KB	81388d53e697ff979d032e1a8985492c9771ce2f1596afe242998ad26efb744b	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\1dc7CK 8O2M4jV0-v99j.lnk.Alphaware	3.59 KB	63b42348d38a4ec2c4fdaf6ad3a9586cabbb65311b39958d413a25b0352e393d	✖
c:\users\keecfmwgj\documents\wo--2pwpxtf.pptx.alphaware	127.05 KB	9f4edea638fee35d3765727e6560453845fa9a2777f9877322bebcb3ac3f2bc8	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RkF0hT0Xfp-m3q.lnk.Alphaware	3.51 KB	127af9db36bb32a49e48b51c835f76ce54a3064cd92e8423c6bfa927bf5c979b	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL.Alphaware	448.99 KB	478cfcf8a6507b6681a2a662d7a263d7811c63fa787c1f66129ad4c3da641b78	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\az80w8eavf6qldtcvji.lnk.alphaware	6.43 KB	b0dd16cfae9e5c7006f200decc883d2fd62cc64e99cbaa910bc6d7df7202c5a1	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\t2V3lQcrptDn.lnk.Alphaware	6.68 KB	8eaf6244a0a7507790fe7b70eb384f38dfb8458a6948f37fe037e49d0e40b625	✖
C:\Users\kEecfMwgj\AppData\Roaming\7ord0oMkDdqdZwcFM7PM.mkv.Alphaware	20.05 KB	06481825a2961641bfc76c058690c6a60147f5e6ffdccbf2056b9888c5d5bf42	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\UgJB0bK8M6Fbzeqf.lnk.Alphaware	3.55 KB	43eefe0e2a255e4cc7842418c87fc3b2b39e6eb83effd45decf39401d15ced55	✖

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\mlaseventheditionofficeonline.xsl.alphaware	332.53 KB	87cf9510fa48ec0e9a7feda861776fcd55192c9e8eefc9ffbd803d47b6f23187	✖
c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\-cj6mviu4.odt.alphaware	91.34 KB	6ed1e5919dc630413bfc51682930e8c983e41c13fd9723ae369cfb978a805556	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini.Alphaware	756 bytes	f8ac4505f5420950c12218e4790337d6dadc653e67b413d9ab7a74088cee4f0b	✖
c:\users\keecfmwgj\links\desktop.lnk.alphaware	820 bytes	738aaa9ae329acdf37c89238b8dd2b46e5f0af608dd9520e7ab470926734eae2	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\dz5o.lnk.alphaware	3.36 KB	2f4014ac00d0dea0856bb71b071a69d5fe2aea0fd80613404857b33d312b58b5	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\Recent\index.dat.Alphaware	244 bytes	1668eea78150c3abb3456043c3a4609bf787c5849482745669cfa40521b1d189	✖
C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQIR\eUSZ\JverrFiKHyZBVDqw.avi.Alphaware	12.20 KB	2a37c8c06cabc7e3780f94fd8abe9a9769b63df33c701316e25ff98f10cd49f7	✖
C:\Users\kEecfMwgj\AppData\Roaming\ObWS3XW5aMy2t2Z9HK.wav.Alphaware	64.34 KB	d8ce0b758dbcb37107dd806dad6f6bad09ef3792ff93c245c9504ec4d3d61f99	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vxbet57toqm.lnk.alphaware	948 bytes	a166cf830d1b42203b61de34726e1a99766d3640b724201b0ee278daf01cded5	✖
c:\users\keecfmwgj\videos\zu2jiwj2ww\iz2buoz_oasw3v_9ugc.flv.alphaware	4.09 KB	28716fb44602efdcc835cda00a66aa81506bee5522fea49a0d28c576a508e2f9	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\k3hqlajeyy.lnk.alphaware	6.66 KB	0898aec6c86dc3c1de26a4f2168655cbdc20bfc8b081346c5105f0d8f29b2a38	✖
C:\Users\Public\Documents\desktop.ini.Alphaware	584 bytes	729828889f47a0dd04bfcdb0c73f87d3e6255abc32ae6996f1c22add01dfae4f	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\miKlgwo4kuAJyz.lnk.Alphaware	4.91 KB	18a248967221412381384494b36176fb9c74317452b9b1b581dbfcc92248f40a	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\qqj69aqvcd-_ggmfehfcj.pdf.lnk.alphaware	3.59 KB	4f78fcdbd0aa2715945ce5be2c6771ca9589914220618ba2134ac445af690320	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\1wwkn7za3pjvj0l2.pdf.lnk.alphaware	6.74 KB	4e32249bab9d8c1d5086e305b774ea99ce7235d27c6e50e106cd706dff185be5	✖
C:\Users\kEecfMwgj\Videos\bleMKBNSsvf5WRB\TVHtwFsg.flv.Alphaware	70.70 KB	24664b3c35667d696aa067190a6f08651c42a99443b1054a17434c48632ffd3c	✖
c:\users\keecfmwgj\documents\daw-ipdr7ovxj2g.docx.alphaware	80.53 KB	7596810f2e7296e596334de523446af1441dfab5bfd8b899a3102b297da851cd	✖
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\nqcf5ew\vmoqizt54\iadqh9.jpg.alphaware	23.82 KB	0a3ab1f865e5280cf78e9e3739f37748da5752950a7d49752ee7874f0a558539	✖
c:\users\keecfmwgj\videos\zu2jiwj2ww\ermdlpgee_opr8.mp4.alphaware	18.47 KB	c13ec530e20be11c0817ce8168bbad9d50c4991cf0c6a16dcd0a5b1c78c4a108	✖
C:\Users\kEecfMwgj\Desktop\fWyG0v4r7alxC.gif.Alphaware	127.41 KB	80d357e6a0e4ede25c9968015fb934c7c6f4f03f52977ff8c818aea55348fca5	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\jnmmi.ots.lnk.alphaware	904 bytes	2d2abc33631ed95a36d5bafee9ce9b939f239066a175cdc709b91454d2abc654	✖
C:\Users\kEecfMwgj\Videos\jvuGC2saBZFJ\8lwQtag2z.swf.Alphaware	66.97 KB	0fbf57404767dcfd0358f8a951466de15157ed419efdd5075c105acd415bcfd6	✖
C:\Users\kEecfMwgj\Documents\y-0\584vk2Slwl33KAWC.docx.Alphaware	133.13 KB	ae1b9a2144b3d41bf9949dfe49300fe82c2392f1ca946e2a1750fe5dfa6c1ec9	✖
C:\Users\kEecfMwgj\Videos\ZShqFxkOqd6c5.mp4.Alphaware	118.43 KB	6f497dfe6f3ba6b1c64ea1add0bbdf59c74da2f4884ce2e39c6b3bf265417602	✖
c:\users\keecfmwgj\videos\jvugc2sabzfj\4_p930hvcz_\bpvw70tznos_6.avi.alphaware	59.84 KB	f58c27f51a897559e46a78b52fa65995f2f859e491177972c67573d3f8b59c67	✖

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\qs1esam6mnjquw3k.lnk.alphaware	1.22 KB	f4516354344abd7f6c69b1f5537a976df05498d2ded74f1b2c677b5e7a22d875	✖
C:\Users\kEecfMwgj\Desktop\IPAZp7HleyfBa.avi.Alphaware	121.53 KB	901fe76d76119f8541e34eca25315dd22026a8fd5f68767eafd7a3b91c98190d	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\cgtmsh0_nmfpfsqohtip.lnk.alphaware	3.43 KB	9aefa6a6f707c0eec0a66a26e9669338659e46f4c603a8f050dcce3691adbf6b	✖
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\sendto\desktop.ini.alphaware	948 bytes	b53d357db181213db373b439f1192de02ceffddbc89fb2deb293b49c018fb18f	✖
C:\Users\kEecfMwgj\Links\OneDrive.lnk.Alphaware	2.20 KB	2bb7672661a96f25db12a0588edf8b9c3f3fc01e1036a7c6c1889172edabcf56	✖
c:\users\keecfmwgj\pictures\w0y6k3cxjraf-y2ue6\jo7fjz3qqw1.gif.alphaware	8.03 KB	1fef2c8f39b3a5e4ef5a9a9bb78f070e7e3b2f1c01370e69c72a60080c8e6618	✖
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\2cvjqDL8AbrH.lnk.Alphaware	1.47 KB	d14b3669cb670533eadfc1f8b07096a1277de39dd199c13810fbc1ce67e279b9	✖
c:\users\keecfmwgj\documents\dz5o.docx.alphaware	58.68 KB	6dbddb11297e934a918caca3b942c4fc102acbe776fbfeb39fa44a0c29173010	✖

Reduced dataset

Host Behavior

Type	Count
Registry	4
Module	1735
Environment	1
User	2
System	216
Process	98
File	5341
Window	3
-	1
Keyboard	2

Process #3: cmd.exe

ID	3
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet & wmic shadowcopy delete
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 108643, Reason: Child Process
Unmonitor End Time	End Time: 151011, Reason: Terminated
Monitor duration	42.37s
Return Code	0
PID	3972
Parent PID	3800
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Environment	16
File	21
Process	2

Process #4: vssadmin.exe

ID	4
File Name	c:\windows\system32\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 108920, Reason: Child Process
Unmonitor End Time	End Time: 149694, Reason: Terminated
Monitor duration	40.77s
Return Code	0
PID	3996
Parent PID	3972
Bitness	64 Bit

Process #5: vssvc.exe

ID	5
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 109414, Reason: RPC Server
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	167.72s
Return Code	Unknown
PID	4024
Parent PID	3996
Bitness	64 Bit

Host Behavior

Type	Count
System	3

Process #7: wmic.exe

ID	7
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic shadowcopy delete
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 148709, Reason: Child Process
Unmonitor End Time	End Time: 150139, Reason: Terminated
Monitor duration	1.43s
Return Code	0
PID	3244
Parent PID	3972
Bitness	64 Bit

Host Behavior

Type	Count
System	7
Module	3
COM	2
Registry	5
File	2
-	1

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 149329, Reason: RPC Server
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	127.80s
Return Code	Unknown
PID	876
Parent PID	3244
Bitness	64 Bit

Process #9: wmiprvse.exe

ID	9
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 149329, Reason: RPC Server
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	127.80s
Return Code	Unknown
PID	3100
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Registry	3
COM	1

Process #10: wmiprvse.exe

ID	10
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 149329, Reason: RPC Server
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	127.80s
Return Code	Unknown
PID	1348
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
Module	4
System	6
Registry	3

Process #11: cmd.exe

ID	11
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 150108, Reason: Child Process
Unmonitor End Time	End Time: 151497, Reason: Terminated
Monitor duration	1.39s
Return Code	0
PID	3400
Parent PID	3800
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Environment	16
File	17
Process	2

Process #12: bcdedit.exe

ID	12
File Name	c:\windows\system32\bcdedit.exe
Command Line	bcdedit /set {default} bootstatuspolicy ignoreallfailures
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 150315, Reason: Child Process
Unmonitor End Time	End Time: 150976, Reason: Terminated
Monitor duration	0.66s
Return Code	0
PID	3396
Parent PID	3400
Bitness	64 Bit

Process #13: bcdedit.exe

ID	13
File Name	c:\windows\system32\bcdedit.exe
Command Line	bcdedit /set {default} recoveryenabled no
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 150411, Reason: Child Process
Unmonitor End Time	End Time: 151207, Reason: Terminated
Monitor duration	0.80s
Return Code	0
PID	3296
Parent PID	3400
Bitness	64 Bit

Process #14: cmd.exe

ID	14
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /C wbadmin delete catalog -quiet
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 150541, Reason: Child Process
Unmonitor End Time	End Time: 152649, Reason: Terminated
Monitor duration	2.11s
Return Code	0
PID	3424
Parent PID	3800
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	10
Process	1

Process #15: wbadmin.exe

ID	15
File Name	c:\windows\system32\wbadmin.exe
Command Line	wbadmin delete catalog -quiet
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 150728, Reason: Child Process
Unmonitor End Time	End Time: 152626, Reason: Terminated
Monitor duration	1.90s
Return Code	0
PID	3464
Parent PID	3424
Bitness	64 Bit

Process #19: notepad.exe

ID	19
File Name	c:\windows\system32\notepad.exe
Command Line	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\kEecfMwgj\AppData\Roaming\readme.txt
Initial Working Directory	C:\Users\kEecfMwgj\AppData\Roaming\
Monitor Start Time	Start Time: 152471, Reason: Child Process
Unmonitor End Time	End Time: 277133, Reason: Terminated by timeout
Monitor duration	124.66s
Return Code	Unknown
PID	2568
Parent PID	3800
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3a2b0d7aa2a94d6d537838a2a18fa25890c2df97c7708e895f7c566f7a65ab76	C:\Users\kEecfMwgj\Desktop\Alphaware.exe, C:\Users\kEecfMwgj\AppData\Roaming\svchost.exe	Dropped File	1078.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
1f07fbece71d67c140a10aa9993f1d5bba5250f21b7cfafcc39e4ea60689223c	C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\readme.txt, C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\readme.txt, C:\Users\kEecfMwgj\Pictures\s... ...C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\NQCf5ew\vmOQizT54\readme.txt, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\readme.txt	Dropped File	1.15 KB	text/plain	Access, Create, Write	SUSPICIOUS
4e9ab5deb85ebedbe89416892dcdc6183edbdf4f9f5458a4c075f8cba8a4e276	C:\Users\kEecfMwgj\AppData\Local\Temp\300wkaa5g.jpg	Dropped File	969.78 KB	image/webp	Access, Create, Write	SUSPICIOUS
647d424bedc754a542ff702c0942983c7770fa53362fb738bd1042984bdb110d	c:\users\keecfmwgj\appdata\roaming\vcnvmrhf2u7xxjbaxrmb.pps.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\vCNVmrhf2U7XXJBaxRmB.pps.Alphaware	Dropped File	70.66 KB	text/plain	Access, Create, Write	CLEAN
5a4efb030996c150529030c7a10e1690fea0d6c2539048c0a60e84a86e36f130	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\4_p930hvcz_.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\4_p930HVcZ_.lnk.Alphaware	Dropped File	4.80 KB	text/plain	Access, Create, Write	CLEAN
ad2a49dd606aa339ca4b319d8a80b1db75ac2d28c651f082610e25f6c97b51b8	c:\users\keecfmwgj\desktop\1yppaa.jpg.alphaware, C:\Users\kEecfMwgj\Desktop\1YPPAA.jpg.Alphaware	Dropped File	3.05 KB	text/plain	Access, Create, Write	CLEAN
e71adbded09bb9f2e3e8f0c7b9affa3f51e7fe80eb1909fc2b65c241a4419853	C:\Users\kEecfMwgj\Documents\UgJB0bK8M6Fbzeqf.xlsx.Alphaware, c:\users\keecfmwgj\documents\ugjb0bk8m6fbzeqf.xlsx.alphaware	Dropped File	52.66 KB	text/plain	Access, Create, Write	CLEAN
2a9b3dacb01d464da3a7e4f99616955b2f99e8a1889dd61fa441200ddb8e9b52	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\y-0.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\y-0.lnk.Alphaware	Dropped File	3.20 KB	text/plain	Access, Create, Write	CLEAN
313de9e8e30738cb15c371b05a23ef7cd38a64a49f1e239eaae4f215f416bb47	c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\az80w8eavf6qldtcvji\r5bauiuaurz 0kbpe.jpg.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\AZ80w8eAVF6qLdtcVJI\r5baulUaurz 0kBPe.jpg.Alphaware	Dropped File	32.97 KB	text/plain	Access, Create, Write	CLEAN
377db872cc28a0df07b74f5fc0bb4a0c94b70226ea066c4df1d4a0e7382b2547	c:\users\keecfmwgj\appdata\roaming\n_rln0z3nrhzqdxj jzi.rtf.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\N_rIN0Z3nRhZqdxj JZI.rtf.Alphaware	Dropped File	14.11 KB	text/plain	Access, Create, Write	CLEAN
931d1667557f0bd9359a3609e9a2642e02a6d1b4188ab9dbf662ad3e42b366cd	C:\Users\kEecfMwgj\Pictures\CGtmsH0_nmfPfsQOHtip\dFW79KlkBOtau4aDuO.jpg.Alphaware, c:\users\keecfmwgj\pictures\cgtmsh0_nmfpfsqohtip\dfw79klkbotau4aduo.jpg.alphaware	Dropped File	35.32 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4a0583e3b0ba5b60eb6b5c3de8402cf2ed92ce8f0fd9b209dcb7301e9cb617cd	c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\iso690nmerical.xsl.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL.Alphaware	Dropped File	283.51 KB	text/plain	Access, Create, Write	CLEAN
7b9865aa930ed83fcba80a30ec990f584e4840d0ac08295051ebeabf21e53684	c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\e1l_xrq6amcgtt.bmp.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\E1l_XrQ6aMcGTT.bmp.Alphaware	Dropped File	73.61 KB	text/plain	Access, Create, Write	CLEAN
ad66744aa3633a14d2935cc338d6714763541707778e22b7a2982b429ad9fcffe	c:\users\keecfmwgj\appdata\roaming\im_qpwmgce7suron0abx.m4a.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Im_qpwMGCe7SuRoN0aBx.m4a.Alphaware	Dropped File	84.99 KB	text/plain	Access, Create, Write	CLEAN
173bd505975005b2ec2170ab50c998622bc452f0ee09df9864bd0961739243d4	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\6jCAQWe-_9EEl7aEUjN.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\6jcaqwe-_9eel7aeujn.lnk.alphaware	Dropped File	1.41 KB	text/plain	Access, Create, Write	CLEAN
087ae75e0a159a72275d09cf544e386d1e6590da85f791c3aa295c6cbc0c043d	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\zR1JJINH15QPReboG.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\zr1jjinh15qprebog.lnk.alphaware	Dropped File	8.61 KB	text/plain	Access, Create, Write	CLEAN
c5b3841d7aca576f0816a28fa54d39b0e61e1553fcc4c8537d40e60259086dd6	c:\users\keecfmwgj\appdata\roaming\s8zdf lucr_z28spu.swf.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\s8ZDF Lucr_Z28Spu.swf.Alphaware	Dropped File	55.78 KB	text/plain	Access, Create, Write	CLEAN
668cc94eb04575d906ec58194389f97d9eb5f3fffb731643433ab33eeb8be6a0	C:\Users\kEecfMwgj\Desktop\UKIs\VP0OeoLUyu0aA\SjIEHWNzBPbEPK.ppt.Alphaware, c:\users\keecfmwgj\desktop\ukIsvp0oeoluyu0aa\sjiehwnzbpbepk.ppt.alphaware	Dropped File	119.76 KB	text/plain	Access, Create, Write	CLEAN
60ab82ccd03da740aef46884a83af55ff6a51a149d82c1ee06601bef8b60764f	C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\k3HQLaJEyY.odp.Alphaware, c:\users\keecfmwgj\documents\y-0\beaeacczbwdfqo39\k3hqlajeyy.odp.alphaware	Dropped File	109.86 KB	text/plain	Access, Create, Write	CLEAN
6e8e90934f9d13fe3028eba01d2c6651b02ebaf182dcb991893afcda991f7e7b	C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\bC7JKZ.swf.Alphaware, c:\users\keecfmwgj\videos\jvugc2sabzfj\bc7jkz.swf.alphaware	Dropped File	115.41 KB	text/plain	Access, Create, Write	CLEAN
7a9caacc4c976f2b317ec7589f209c1cf22b9b645cc6045bb69872a1e9e243c5	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\egl9rx1kxsqwh.mkv.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\EGL9Rx1KXSqWh.mkv.lnk.Alphaware	Dropped File	1.47 KB	text/plain	Access, Create, Write	CLEAN
88224add061e5303e3776f409ec980ccdd0f13a56f72768a7b036a5011a60589	c:\users\public\videos\sample videos\wildlife.wmv.alphaware, C:\Users\Public\Videos\Sample Videos\Wildlife.wmv.Alphaware	Dropped File	10240.00 KB	text/plain	Access, Create, Write	CLEAN
206c87ba6f0fdb1c2ad3eecf95d99af73ac4762a6f62b7768467407cfea182ae	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vo9mo3eeu2slpqjwfm.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Vo9MO3eEU2 SLpQJWfM.lnk.Alphaware	Dropped File	5.30 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5310fb2e5c77a90243ef2c5d8c43b2e8d2bc140e5a5ea64c79ea4d11015b9c07	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\h8wehqdt-nllywl7w3.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\H8WEhqDt-nLLYwL7w3.lnk.Alphaware	Dropped File	5.30 KB	text/plain	Access, Create, Write	CLEAN
70bd7d4a2dcb825aa8bcf0ad2a353c9be79676a02e434190ab91a3c1c956674a	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vmoqjzt54.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\vmOQizT54.lnk.Alphaware	Dropped File	8.01 KB	text/plain	Access, Create, Write	CLEAN
014da00ff1825e399bac0e5f12f172b98af0577a15cfc89e024585ef500ed2af	c:\users\keecfmwgj\appdata\roaming\bnr8t.csv.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\bNR8T.csv.Alphaware	Dropped File	68.74 KB	text/plain	Access, Create, Write	CLEAN
1332129f0c4cb2e754a05843eda9390a336d128b4cc3d38adc34b8204a1baad9	c:\users\keecfmwgj\desktop\cz6ivaatp9f8.m4a.alphaware, C:\Users\kEecfMwgj\Desktop\cZ6ivAAtP9f8.m4a.Alphaware	Dropped File	83.68 KB	text/plain	Access, Create, Write	CLEAN
ed92bbba46d682a29678f2baa60667cf2b16828caa597037ab06c2d2d31db339	C:\Users\kEecfMwgj\Videos\jvuGC2saBZFJ\MADiRK5BENdO7pHH.flv.Alphaware, c:\users\keecfmwgj\videos\jvugc2sabzfj\madirk5bendo7phh.flv.alphaware	Dropped File	4.78 KB	text/plain	Access, Create, Write	CLEAN
2d25226ca002e584ab1b0d10b7dd311f6d646da5f95c88fe4a39fb4939abf526	C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\pOajqkURwLncz.wav.Alphaware, c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\poajqkurwlncz.wav.alphaware	Dropped File	130.61 KB	text/plain	Access, Create, Write	CLEAN
4c8fa0396fd2a61e07bc2813a2c2e2e2eb22089a2fef40b0957c61bb8852ddf0	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent_aoxubo1xfzs.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent_aOXubo1XFZS.lnk.Alphaware	Dropped File	3.49 KB	text/plain	Access, Create, Write	CLEAN
deeefaba22ffd6bf20007e1cb993c49ddd6ac0f25d8bcb4cb8107466c85cdb7d	c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\jc7ce.wav.alphaware, C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\Jc7CE.wav.Alphaware	Dropped File	77.09 KB	text/plain	Access, Create, Write	CLEAN
883389249f9db96cb607065a08ad0edb3adfc430e3534cf93b03604d8d8b246c	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\w0y6k3cxjraf-y2ue6.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\w0y6K3cxjraf-y2uE6.lnk.Alphaware	Dropped File	3.38 KB	text/plain	Access, Create, Write	CLEAN
c29e95222f1f7b69c4a49c510f4e9e18b808556caac61e7703ebbdb02fcddbae	c:\users\keecfmwgj\desktop\wqtdeefonuz7kxbdbx.pps.alphaware, C:\Users\kEecfMwgj\Desktop\WQTdEEFonuZ7KxbDBX.pps.Alphaware	Dropped File	20.05 KB	text/plain	Access, Create, Write	CLEAN
19645284663 28e1f4a269d6868f2189118d227d2a2ae77eb0fd10314f5b77ce8	c:\users\keecfmwgj\appdata\roaming\egl9rx1kxsqwh.mkv.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\EGL9Rx1KXSqWh.mkv.Alphaware	Dropped File	41.24 KB	text/plain	Access, Create, Write	CLEAN
82aebf50d58b108d2cc2d316671e0bea8aad7d07b93f1c3a66cb3e2f79e2bc2a	c:\users\keecfmwgj\documents\d_cm4s7fp.pptx.alphaware, C:\Users\kEecfMwgj\Documents\D_cm4s7fP.pptx.Alphaware	Dropped File	40.49 KB	text/plain	Access, Create, Write	CLEAN
74020efa349c1f6fc36e7341874bb6d3442cc5113100018aa3751e88593a3f29	c:\users\keecfmwgj\appdata\roaming\nbyvlogs.m4a.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\NbYVLogs.m4a.Alphaware	Dropped File	128.55 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d1ef917db973ca1597d744e94d8f0ae35a7527cf10231dbf559412630313937d	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\nqr9nqmjn0i.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\NqR9nQMJn0 I.lnk.Alphaware	Dropped File	6.34 KB	text/plain	Access, Create, Write	CLEAN
deedee1a4c21146b82c3747bfc1147e63003f65a8221122ab44f6c6e0e7136ea	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\eusz.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\eUSZ.lnk.Alphaware	Dropped File	6.18 KB	text/plain	Access, Create, Write	CLEAN
27e59fa0f2f5b8e750198cf15921267d930b26a2dadade7ad244f5b7ffe37254	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\e4w8io-jmf.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\e4W8iO-jmf.lnk.Alphaware	Dropped File	4.68 KB	text/plain	Access, Create, Write	CLEAN
87452060df99e73d3b29c5d6746c362eb7dbcd27198c9f474e460d5bd85d29a0	c:\users\keecfmwgj\pictures\sd_mf\96isf-4zdjysw7lw.png.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\96IsF-4ZdJysw7LW.png.Alphaware	Dropped File	12.91 KB	text/plain	Access, Create, Write	CLEAN
5d8b8bbdd997b313b5c953d6e5926cde314913f860c205768de4609f7f5af38c	C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\Jl GdXo.wav.Alphaware, c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\jl gdxo.wav.alphaware	Dropped File	119.93 KB	text/plain	Access, Create, Write	CLEAN
7781c693865e7d9a548cbedd790cebfb7eabb9de186616b918d76ba78075566b	c:\users\keecfmwgj\videos\zdm5mb5uma.avi.alphaware, C:\Users\kEecfMwgj\Videos\zdm5mb5UMA.avi.Alphaware	Dropped File	84.22 KB	text/plain	Access, Create, Write	CLEAN
a98112f44d6dc1a1a2692b89c6a8f030407fc1120ffa539da3732a195d0b6ea0	c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\chicago.xsl.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL.Alphaware	Dropped File	386.95 KB	text/plain	Access, Create, Write	CLEAN
140b0484da5f7937a9be1fe923ec2c1d134adc98b7391887a64300fb6b890362	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\bIeMKBNSsvf5WRB.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\biemkbnssvf5wrb.lnk.alphaware	Dropped File	3.30 KB	text/plain	Access, Create, Write	CLEAN
7657d3b36626d1f25a9b10f020aa5e7c3a2863e1cd3478d5628c68d4c0854561	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\v8u50bnoh.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\V8U50BNOH.lnk.Alphaware	Dropped File	6.49 KB	text/plain	Access, Create, Write	CLEAN
925f8cf001c8b395912cfbd3a4a15752636a4f114508c172ce37a3040d3019b1	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\ieee2006officeonline.xsl.alphaware	Dropped File	383.70 KB	text/plain	Access, Create, Write	CLEAN
4b7cb1d030155aa2776fb7ecac443b0ffaa2ea145982127a6319350ea9de0275	C:\Users\kEecfMwgj\Desktop\j99Z9MOpk.pdf.Alphaware, c:\users\keecfmwgj\desktop\j99z9mopk.pdf.alphaware	Dropped File	86.16 KB	text/plain	Access, Create, Write	CLEAN
7293fef9c6a5654fe059791b1dfcb399a4da07bf79c99a81533e5914db95e5f9	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RBnxFLdoe6j5FMDq.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\rbnxfldoe6j5fmdq.lnk.alphaware	Dropped File	3.30 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
01e8f85a450cb53b54fa1035f74b303913fd9806495248f1fde069b1cb1ac99	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\MKqMrJd2GayW Iyftd.ots.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\mkqmrjd2gayw iyftd.ots.lnk.alphaware	Dropped File	3.51 KB	text/plain	Access, Create, Write	CLEAN
b11d6fbdbd5e1594b46d24c8e16d7d0b09478bcf8c90cbf613c41a00a650d619	C:\Users\kEecfMwgj\Desktop\desktop.ini.Alphaware, c:\users\keecfmwgj\desktop\desktop.ini.alphaware	Dropped File	584 bytes	text/plain	Access, Create, Write	CLEAN
7a4f65b27831e3636dfc22966ff1468bca0097a40c332d89520f9ad9d3fc3c44	c:\users\keecfmwgj\appdata\roaming\z2r-dghdhevsmryotz.mp3.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\z2r-DGhdhEVsMRYoTz.mp3.Alphaware	Dropped File	106.70 KB	text/plain	Access, Create, Write	CLEAN
6a0833ab6a5d3205cf31df709ebc65de77cebf9a95ebcdd4401b93ee26117165	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\ozdqhhdycahwn.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\ozdQhhdYCAhwn.lnk.Alphaware	Dropped File	3.49 KB	text/plain	Access, Create, Write	CLEAN
84e587044e798fd3d6b401b23a568d89d5be4c7d4bb874f13baa6cf149bb4563	c:\users\keecfmwgj\pictures\q_m8xgrwlwvpa_ok jpb.jpg.alphaware, C:\Users\kEecfMwgj\Pictures\q_m8XgrWlwVpa_ok Jpb.jpg.Alphaware	Dropped File	94.28 KB	text/plain	Access, Create, Write	CLEAN
081de4eaf8fe463b0b6f39224690fb73c1e9e5fb996333640d25dcaa2af1a18f	C:\Users\kEecfMwgj\Desktop\c-jf0ya1RIcN.mp4.Alphaware, c:\users\keecfmwgj\desktop\c-jf0ya1ricn.mp4.alphaware	Dropped File	47.95 KB	text/plain	Access, Create, Write	CLEAN
99d430a38a82ad70c686c4273d85bac48d5918b942f4969e56265a705cf16a78	C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\4_p930HVcZ_\c4x.flv.Alphaware, c:\users\keecfmwgj\videos\jvugc2sabzfj\4_p930hvcz_\c4x.flv.alphaware	Dropped File	112.28 KB	text/plain	Access, Create, Write	CLEAN
701414085c3180dd5e1513ed8a5e196be6abf2d1c7e565db9cf11f923668ee9d	c:\users\keecfmwgj\pictures\desktop.ini.alphaware, C:\Users\kEecfMwgj\Pictures\desktop.ini.Alphaware	Dropped File	884 bytes	text/plain	Access, Create, Write	CLEAN
f04aecab34f432b855a6bb815f8688692b1be169b549af2336663276841e5322	C:\Users\kEecfMwgj\Music\JtwiWA.m4a.Alphaware, c:\users\keecfmwgj\music\jtwiwa.m4a.alphaware	Dropped File	23.80 KB	text/plain	Access, Create, Write	CLEAN
b446e67d96853bfb56189698130157393b2d538eefebc8da56305f0ad97329d8	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\dFW79KlkBOtau4aDuO.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\dfw79klkbotau4aduo.lnk.alphaware	Dropped File	5.30 KB	text/plain	Access, Create, Write	CLEAN
f8bc15b261895fe111366d04df687c6ff8d5c4b3b726ee9641c8e32cc01c8401	C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQlR\eUSZ\awU7DFoRrK67OUHE2Uat.mp4.Alphaware, c:\users\keecfmwgj\videos\zu2jiwj2ww\yqlr\eusz\awu7dforrk67ouhe2uat.mp4.alphaware	Dropped File	128.53 KB	text/plain	Access, Create, Write	CLEAN
91c2ade52e5c75e713a8d85dee590ce61563a39b5346feae931b1e9346c1db82	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Cookies\keecfmwgj@login.microsoftonline[2].txt.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\cookies\keecfmwgj@login.microsoftonline[2].txt.alphaware	Dropped File	756 bytes	text/plain	Access, Create, Write	CLEAN
ac2dd5075ba5a47d6e9bd1d60469d45ed244bc90f407a7706fa7bc1c1a6155b9	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\roaming.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Roaming.lnk.Alphaware	Dropped File	1.18 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c538c278ef89ca7befb259bb22e8ace75474a3253723504463023487 67f92010	C:\Users\kEecfMwgj\Contacts\desktop.ini.Alphaware, c:\users\keecfmwgj\contacts\desktop.ini.alphaware	Dropped File	756 bytes	text/plain	Access, Create, Write	CLEAN
78d5dafdeea54a2bae733365873a2212d6d04379fe6284a79f2a61c9ed3a3579	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\bffgcaoao_f0b_.swf.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\BfFgcaOAo_F0B_.swf.lnk.Alphaware	Dropped File	4.93 KB	text/plain	Access, Create, Write	CLEAN
e2411e9ce863c7b4d347408e994bd5e2b905d21350db863d6a13133211eaf1ff	C:\Users\kEecfMwgj\Music\5jdQ8S\t3tMVJXbAaJh1K.mp3.Alphaware, c:\users\keecfmwgj\music\5jdq8s\t3tmvjxbaajh1k.mp3.alphaware	Dropped File	51.26 KB	text/plain	Access, Create, Write	CLEAN
54bb466e7a682006b523c0e39f54355f55d51fd6473a0f4281bf421ea0381bf2	C:\Users\kEecfMwgj\Desktop\8-6P.wav.Alphaware, c:\users\keecfmwgj\desktop\8-6p.wav.alphaware	Dropped File	132.45 KB	text/plain	Access, Create, Write	CLEAN
b1a87382f1870b618aba80572827bd4bc22384163896b45301ffac77ebd141bd	c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\onrpsaekvylzpjqzcm2l.mkv.alphaware, C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\OnrpsaEkvylzPJqZCM2l.mkv.Alphaware	Dropped File	2.07 KB	text/plain	Access, Create, Write	CLEAN
52b121d159493b1614379294dae7d6e0788be7d71db5a5355ccbad849825f609	C:\Users\kEecfMwgj\Music\5jdQ8S\hX1YQpkZK 4fEglyKr.mp3.Alphaware, c:\users\keecfmwgj\music\5jdq8s\hx1yqpkzk 4feglykr.mp3.alphaware	Dropped File	133.47 KB	text/plain	Access, Create, Write	CLEAN
312fef44dad6a75a8bf7908b969fe9195f0569b3bc7e836c08d86521dc7bdc45	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\tvhtwfsg.flv.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\TVHtwFsg.flv.lnk.Alphaware	Dropped File	4.95 KB	text/plain	Access, Create, Write	CLEAN
853ec114bb1050fb0950e428e0ef78c47673ccb40720a17088b36fdde69906e9f	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\NQCf5ew.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\nqcf5ew.lnk.alphaware	Dropped File	6.26 KB	text/plain	Access, Create, Write	CLEAN
fa3acd99f3a83d43efcb2df96455e08ef3befaee63a918aeb0b2f05421e9aad1	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\4a87c_8npb.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\4A87C_8NPb.lnk.Alphaware	Dropped File	3.45 KB	text/plain	Access, Create, Write	CLEAN
22b5c0695bf5fd512e62706caff6cc51d0191b72fe88b29b0804a66437890703	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\96isf-4zdjysw7lw.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\96IsF-4ZdJysw7LW.lnk.Alphaware	Dropped File	4.93 KB	text/plain	Access, Create, Write	CLEAN
b44c9ef9bf219eacfb5f515ec071c383fc461382646c8e0e239aaf0088b06dd8	C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\1tTeAH3Idl9j.m4a.Alphaware, c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\1tteah3idl9j.m4a.alphaware	Dropped File	102.18 KB	text/plain	Access, Create, Write	CLEAN
a5ac8e5a2200ab118f0db0e52611ae22560314021d4fc9d2585b635066f2d3c4	c:\users\keecfmwgj\documents\o4vmeo_pmk30fk6.xlsx.alphaware, C:\Users\kEecfMwgj\Documents\O4VMeO_PmK30fk6.xlsx.Alphaware	Dropped File	13.95 KB	text/plain	Access, Create, Write	CLEAN
34bcaf8fb00efe56b1c060041773689a44c190eccdda9adea2217550b6c5b510	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\TKqjZN.flv.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\tkqjzn.flv.lnk.alphaware	Dropped File	4.80 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
72c12a955553bd1afa872321069078c97e1c5c03b830b13e89b6921704056c57	c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\shows desktop.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk.Alphaware	Dropped File	608 bytes	text/plain	Access, Create, Write	CLEAN
8af6fb49b17eaaed2fa3f4cf431d04af654cefabbc6973793a9cbb7a999133c3	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\oaaqqjrx6y_jtlap6.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\oaaQQjrX6y_jTlap6.lnk.Alphaware	Dropped File	992 bytes	text/plain	Access, Create, Write	CLEAN
04a2f40e8311cf9fc611869c82ea2ce3da5a391a62410d01a59f598b28dcdaa4	c:\users\keecfmwgj\desktop\mngjsodzb1khxmh.mp4.alphaware, C:\Users\kEecfMwgj\Desktop\MNGJsodzb1khxMh.mp4.Alphaware	Dropped File	20.76 KB	text/plain	Access, Create, Write	CLEAN
a89e973014b0dd3c75a4fd8b606310f39e8bb025b345a6008e7038d5522749d7	c:\users\keecfmwgj\appdata\roaming\uk0_t4zjwac.wav.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\UK0_T4zjWaC.wav.Alphaware	Dropped File	41.24 KB	text/plain	Access, Create, Write	CLEAN
8d507f71fc8cf794b011e6f89540b5f259823f2dc4ed747ff8555c1c20944634	C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\AZ80w8eAVF6qLdtcVJI\zR1JJINH15QPRebоG.png.Alphaware, c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\az80w8eavf6qldtcvji\zr1jjinh15qprebog.png.alphaware	Dropped File	76.99 KB	text/plain	Access, Create, Write	CLEAN
4db6323b8870408c05fb4a201ab98f2138550e930b8ff64cd6ea4fd383b4d669	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\apasixthedition officeonline.xsl.alphaware	Dropped File	434.59 KB	text/plain	Access, Create, Write	CLEAN
1568ecdbdb04ae12543d3503e6ef1429c56711e7fa47b9fafc54cbd4ceefbd33	c:\users\keecfmwgj\music\5jdq8s\zmtegoau5-f.wav.alphaware, C:\Users\kEecfMwgj\Music\5jdQ8S\zMtEGOAU5-f.wav.Alphaware	Dropped File	81.34 KB	text/plain	Access, Create, Write	CLEAN
7680cd3936aa709277bbb3728202f45821e0b636267513d777aa4056235cecb7	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\te-nh.flv.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\te-nH.flv.lnk.Alphaware	Dropped File	1.41 KB	text/plain	Access, Create, Write	CLEAN
1b6e4acceb33696e532f3d7cd556eb6d86d812ac176299e40ea52663adddf77f	C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\LljGz_b-guf6pPz.wav.Alphaware, c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\lijgz_b-guf6ppz.wav.alphaware	Dropped File	59.30 KB	text/plain	Access, Create, Write	CLEAN
db3f053ea4f54eda35e451a115d6633cda8c38fa23dfa55512fdd7f18efd7a0f	C:\Users\kEecfMwgj\Desktop\mxWMxpSlb1Z2y3xfhO0.swf.Alphaware, c:\users\keecfmwgj\desktop\mxwmxpslb1z2y3xfho0.swf.alphaware	Dropped File	76.26 KB	text/plain	Access, Create, Write	CLEAN
080496dffcb29b25c5351a0373aa161589bd3fde67be5775093e742db4eac6e9	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\9wzxgia1p9.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\9WZXgiA1p9.lnk.Alphaware	Dropped File	4.86 KB	text/plain	Access, Create, Write	CLEAN
795908a0821f809e827b118e179138a434a3f17b0e56fc246de9f197c7080c3b	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\sD_Mf.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\sd_mf.lnk.alphaware	Dropped File	3.20 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cb2b7b7fc8ba818db9c65059f42b6c7a6546e068ebd77b7da4ce404e5357f7c5	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\7cu9qgyf.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\7Cu9qgyf.lnk.Alphaware	Dropped File	6.61 KB	text/plain	Access, Create, Write	CLEAN
b939cf5cd0e6c95ceb0bafb15a780e8050420bc31a675b60f00e5bb5d574e475	C:\Users\kEecfMwgj\AppData\Roaming\t2oMmxPi.flv.Alphaware, c:\users\keecfmwgj\appdata\roaming\t2ommxpi.flv.alphaware	Dropped File	75.26 KB	text/plain	Access, Create, Write	CLEAN
5644fcd3e7d867179b50f5f288cb63e519d0720195ce58674b886cc7ec87bcb8	c:\users\keecfmwgj\documents\y-0\beaeacczbwdfqo39\kxx8q7znvev6faidqyx.xlsx.alphaware, C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\kxX8q7znVEV6F AiDQyX.xlsx.Alphaware	Dropped File	64.43 KB	text/plain	Access, Create, Write	CLEAN
6a642840f89898869706bf05374ae335ad25b67ee32dcc5a441c94c1c7bf7536	c:\users\keecfmwgj\appdata\roaming\2cvjqdl8abrh.rtf.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\2cvjqDL8AbrH.rtf.Alphaware	Dropped File	113.99 KB	text/plain	Access, Create, Write	CLEAN
9c1327904e184c164a59335ada2cdfe03e09ac1ce1f8b95de1ce145e917faece	c:\users\keecfmwgj\desktop\mkpzbzgpkyhpvsxosep3.mp3.alphaware, C:\Users\kEecfMwgj\Desktop\MKPZbzGpKYHPVsXosEp3.mp3.Alphaware	Dropped File	37.36 KB	text/plain	Access, Create, Write	CLEAN
80055bedc01c07d618e091109c8f42ba78100d070d609d4f1524eceff97a67cf	c:\users\keecfmwgj\links\recentplaces.lnk.alphaware, C:\Users\kEecfMwgj\Links\RecentPlaces.lnk.Alphaware	Dropped File	692 bytes	text/plain	Access, Create, Write	CLEAN
3fbdad8e1dc18b41fb570a3cb173ad32e8e7ede0c6bcd67d7ff6613bebe38697	C:\Users\kEecfMwgj\Music\8wsZ\sRZM.m4a.Alphaware, c:\users\keecfmwgj\music\8wsz\srzm.m4a.alphaware	Dropped File	100.74 KB	text/plain	Access, Create, Write	CLEAN
e402b6a03f67110975fd6df62a7e72c8e3a267951543719fcef7605d129210d0	c:\users\keecfmwgj\videos\jvugc2sabzfj\0o6jwd.mp4.alphaware, C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\0o6jwd.mp4.Alphaware	Dropped File	60.36 KB	text/plain	Access, Create, Write	CLEAN
1d212a645ef441eadf3d11529bed8eba5a963197ba9ec9d5f50a2c73663e1872	C:\Users\kEecfMwgj\Documents\1dc7CK 8O2M4jV0-v99j.doc.Alphaware, c:\users\keecfmwgj\documents\1dc7ck 8o2m4jv0-v99j.doc.alphaware	Dropped File	24.05 KB	text/plain	Access, Create, Write	CLEAN
badc04a6c6894af1b0b1a21ae9c7b72b947cbd6bf243d45d0ac92d5f26ae7003	C:\Users\kEecfMwgj\Videos\0vDMTR303fbv.avi.Alphaware, c:\users\keecfmwgj\videos\0vdmtr303fbv.avi.alphaware	Dropped File	83.38 KB	text/plain	Access, Create, Write	CLEAN
4b136cc0e370df5b17ad076b661dce603f0b61b00a6a2253a4df4ab240fff92f	C:\Users\kEecfMwgj\Documents\y-0\z8zS.rtf.Alphaware, c:\users\keecfmwgj\documents\y-0\z8zs.rtf.alphaware	Dropped File	96.41 KB	text/plain	Access, Create, Write	CLEAN
dfabf4334aee5ed2a34fa05c3409bef441bb8176eb0bf5c05f1feb8f23b0333b	c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\v8u50bnoh.bmp.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\V8U50BNOH.bmp.Alphaware	Dropped File	127.03 KB	text/plain	Access, Create, Write	CLEAN
c8251fb5b793785e6a1d6c592a17046c2ab012644c1975e7e79634b3175799ff	c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\mlvaw3l8e0fmzi-r4q.gif.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\mlVaW3l8E0FMzi-R4q.gif.Alphaware	Dropped File	110.99 KB	text/plain	Access, Create, Write	CLEAN
0030e291131fe9e00e6658e67969401b1d63b1579a80d7b3c6e2fcbf933c93df	c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\windows media player.lnk.alphaware... ...C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk.Alphaware	Dropped File	2.22 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
81e080a6d94c56585dd6fad29bcb4a2f5e73b031a562cd57e3ba7ae0d42e24ee	C:\Users\kEecfMwgj\Searches\desktop.ini.Alphaware, c:\users\keecfmwgj\searches\desktop.ini.alphaware	Dropped File	904 bytes	text/plain	Access, Create, Write	CLEAN
9fdab2d83f2d480c414f22057e931ae5269a512f4ff3f97257eeb29859e2b725	C:\Users\kEecfMwgj\Music\8wsZ\vGw-gK7bU.mp3.Alphaware, c:\users\keecfmwgj\music\8wsz\vgw-gk7bu.mp3.alphaware	Dropped File	55.70 KB	text/plain	Access, Create, Write	CLEAN
671ead14985a314c03d5b144cb0d789e967081b9da840a86a28183bca7c9f68c	C:\Users\kEecfMwgj\Documents_aOXubo 1XFZS.docx.Alphaware, c:\users\keecfmwgj\documents_aoxubo 1xfzs.docx.alphaware	Dropped File	70.41 KB	text/plain	Access, Create, Write	CLEAN
96038f172abd4300b60a7eb2d8d024ef35010786e38ac144e12166700cc9ee22	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\MADiRK5BENdO7pHH.flv.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\madirk5bendo7phh.flv.lnk.alphaware	Dropped File	5.01 KB	text/plain	Access, Create, Write	CLEAN
005895ea100e66ac1b752aec86e025267391b625df32c934bda8ce57bb098c09	C:\Users\kEecfMwgj\AppData\Roaming\AcoFPdLUL2Wyq3ljkzb.jpg.Alphaware, c:\users\keecfmwgj\appdata\roaming\acofpdlul2wyq3ljkzb.jpg.alphaware	Dropped File	108.61 KB	text/plain	Access, Create, Write	CLEAN
a2c0580d6653d755cd72893416ad3c5ad4f185829e2a29152abd7fb5964ac057	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\7ord0oMkDdqdZwcFM7PM.mkv.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\7ord0omkddqdzwcfm7pm.mkv.lnk.alphaware	Dropped File	1.51 KB	text/plain	Access, Create, Write	CLEAN
4a34518459689352942bc2d5824a79057f4a22577e9038c336451ad297152c69	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\bJTM1.flv.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\bjtm1.flv.lnk.alphaware	Dropped File	6.55 KB	text/plain	Access, Create, Write	CLEAN
c16813818833d936754c4c985250971a07b6e12483e158c14a24cbcb34826787	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\hWvMFQJJJ.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\hwvmfqjjj.lnk.alphaware	Dropped File	3.22 KB	text/plain	Access, Create, Write	CLEAN
69a605a483b58d7ecc864dd6313dc3f1c679742d56bda131e44651d4bd7bd54e	C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\eRiABnWG9I.m4a.Alphaware, c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\eriabnwg9i.m4a.alphaware	Dropped File	83.74 KB	text/plain	Access, Create, Write	CLEAN
81388d53e697ff979d032e1a8985492c9771ce2f1596afe242998ad26efb744b	c:\users\keecfmwgj\appdata\roaming\wy-il 75unfs8bktr.wav.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\wY-iL 75UNFS8BKTR.wav.Alphaware	Dropped File	114.30 KB	text/plain	Access, Create, Write	CLEAN
63b42348d38a4ec2c4fdaf6ad3a9586cabbb65311b39958d413a25b0352e393d	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\1dc7CK8O2M4jV0-v99j.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\1dc7ck8o2m4jv0-v99j.lnk.alphaware	Dropped File	3.59 KB	text/plain	Access, Create, Write	CLEAN
9f4edea638fee35d3765727e6560453845fa9a2777f9877322bebcb3ac3f2bc8	c:\users\keecfmwgj\documents\wo--2pwpxtf.pptx.alphaware, C:\Users\kEecfMwgj\Documents\wO--2PwPxtF.pptx.Alphaware	Dropped File	127.05 KB	text/plain	Access, Create, Write	CLEAN
127af9db36bb32a49e48b51c835f76ce54a3064cd92e8423c6bfa927bf5c979b	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RkF0hT0Xfp-m3q.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\rkf0ht0xfp-m3q.lnk.alphaware	Dropped File	3.51 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
478cfcf8a6507b6681a2a662d7a263d7811c63fa787c1f66129ad4c3da641b78	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\turabian.xsl.alphaware	Dropped File	448.99 KB	text/plain	Access, Create, Write	CLEAN
b0dd16cfae9e5c7006f200decc883d2fd62cc64e99cbaa910bc6d7df7202c5a1	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\az80w8eavf6qldtcvji.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\AZ80w8eAVF6qLdtcVJI.lnk.Alphaware	Dropped File	6.43 KB	text/plain	Access, Create, Write	CLEAN
8eaf6244a0a7507790fe7b70eb384f38dfb8458a6948f37fe037e49d0e40b625	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\t2V3lQcrptDn.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\t2v3iqcrptdn.lnk.alphaware	Dropped File	6.68 KB	text/plain	Access, Create, Write	CLEAN
06481825a2961641bfc76c058690c6a60147f5e6ffdccbf2056b9888c5d5bf42	C:\Users\kEecfMwgj\AppData\Roaming\7ord0oMkDdqdZwcFM7PM.mkv.Alphaware, c:\users\keecfmwgj\appdata\roaming\7ord0omkddqdzwcfm7pm.mkv.alphaware	Dropped File	20.05 KB	text/plain	Access, Create, Write	CLEAN
43eefe0e2a255e4cc7842418c87fc3b2b39e6eb83effd45decf39401d15ced55	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\UgJB0bK8M6FbzeqF.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\ugjb0bk8m6fbzeqf.lnk.alphaware	Dropped File	3.55 KB	text/plain	Access, Create, Write	CLEAN
87cf9510fa48ec0e9a7feda861776fcd55192c9e8eefc9ffbd803d47b6f23187	c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\mlaseventheditionofficeonline.xsl.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl.Alphaware	Dropped File	332.53 KB	text/plain	Access, Create, Write	CLEAN
6ed1e5919dc630413bfc51682930e8c983e41c13fd9723ae369cfb978a805556	c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\-cj6mviu4.odt.alphaware, C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\-Cj6mvIu4.odt.Alphaware	Dropped File	91.34 KB	text/plain	Access, Create, Write	CLEAN
f8ac4505f5420950c12218e4790337d6dadc653e67b413d9ab7a74088cee4f0b	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\desktop.ini.alphaware	Dropped File	756 bytes	text/plain	Access, Create, Write	CLEAN
738aaa9ae329acdf37c89238b8dd2b46e5f0af608dd9520e7ab470926734eae2	c:\users\keecfmwgj\links\desktop.lnk.alphaware, C:\Users\kEecfMwgj\Links\Desktop.lnk.Alphaware	Dropped File	820 bytes	text/plain	Access, Create, Write	CLEAN
2f4014ac00d0dea0856bb71b071a69d5fe2aea0fd80613404857b33d312b58b5	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\dz5o.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\DZ5O.lnk.Alphaware	Dropped File	3.36 KB	text/plain	Access, Create, Write	CLEAN
1668eea78150c3abb3456043c3a4609bf787c5849482745669cfa40521b1d189	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\Recent\index.dat.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\office\recent\index.dat.alphaware	Dropped File	244 bytes	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2a37c8c06cabc7e3780f94fd8abe9a9769b63df33c701316e25ff98f10cd49f7	C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQlR\eUSZ\JverrFiKHyZBVDqw.avi.Alphaware, c:\users\keecfmwgj\videos\zu2jiwj2ww\yqlr\eusz\jverrfikhyzbvdqw.avi.alphaware	Dropped File	12.20 KB	text/plain	Access, Create, Write	CLEAN
d8ce0b758dbcb37107dd806dad6f6bad09ef3792ff93c245c9504ec4d3d61f99	C:\Users\kEecfMwgj\AppData\Roaming\ObWS3XW5aMy2t2Z9HK.wav.Alphaware, c:\users\keecfmwgj\appdata\roaming\obws3xw5amy2t2z9hk.wav.alphaware	Dropped File	64.34 KB	text/plain	Access, Create, Write	CLEAN
a166cf830d1b42203b61de34726e1a99766d3640b724201b0ee278daf01cded5	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vxbet57toqm.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Vxbet57tOqM.lnk.Alphaware	Dropped File	948 bytes	text/plain	Access, Create, Write	CLEAN
28716fb44602efdcc835cda00a66aa81506bee5522fea49a0d28c576a508e2f9	c:\users\keecfmwgj\videos\zu2jiwj2ww\iz2b uoz_oasw3v_9ugc.flv.alphaware, C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\iZ2B uOZ_oASw3v_9uGC.flv.Alphaware	Dropped File	4.09 KB	text/plain	Access, Create, Write	CLEAN
0898aec6c86dc3c1de26a4f2168655cbdc20bfc8b081346c5105f0d8f29b2a38	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\k3hqlajeyy.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\k3 HQLaJEyY.lnk.Alphaware	Dropped File	6.66 KB	text/plain	Access, Create, Write	CLEAN
729828889f47a0dd04bfcdb0c73f87d3e6255abc32ae6996f1c22add01dfae4f	C:\Users\Public\Documents\desktop.ini.Alphaware, c:\users\public\documents\desktop.ini.alphaware	Dropped File	584 bytes	text/plain	Access, Create, Write	CLEAN
18a24896722141238138449 4b36176fb9c74317452b9b1b581dbfcc92248f40a	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\miKlgwo4kuAJyz.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\miklgwo4kuajyz.lnk.alphaware	Dropped File	4.91 KB	text/plain	Access, Create, Write	CLEAN
4f78fcdbd0aa2715945ce5be2c6771ca9589914220618ba2134ac445af690320	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\qq69aqvcd-_ggmfehfcj.pdf.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\qQ69AqvCd-_gGmFEhfCj.pdf.lnk.Alphaware	Dropped File	3.59 KB	text/plain	Access, Create, Write	CLEAN
4e32249bab9d8c1d5086e305b774ea99ce7235d27c6e50e106cd706dff185be5	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\1wwkn7za3pjvj0l2.pdf.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\1wWkN7zA3pJvJ0l2.pdf.lnk.Alphaware	Dropped File	6.74 KB	text/plain	Access, Create, Write	CLEAN
24664b3c35667d696aa067190a6f08651c42a99443b1054a17434c48632ffd3c	C:\Users\kEecfMwgj\Videos\bIeMKBNSsvf5WRB\TVHtwFsg.flv.Alphaware, c:\users\keecfmwgj\videos\biemkbnssvf5wrb\tvhtwfsg.flv.alphaware	Dropped File	70.70 KB	text/plain	Access, Create, Write	CLEAN
7596810f2e7296e596334de523446af1441dfab5bfd8b899a3102b297da851cd	c:\users\keecfmwgj\documents\daw-ipdr7ovxj2g.docx.alphaware, C:\Users\kEecfMwgj\Documents\Daw-ipdR7oVXj2G.docx.Alphaware	Dropped File	80.53 KB	text/plain	Access, Create, Write	CLEAN
0a3ab1f865e5280cf78e9e3739f37748da5752950a7d49752ee7874f0a558539	c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\nqcf5ew\vmoqizt54\iadqh9.jpg.alphaware, C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\NQCf5ew\vmOQizT54\IaDqH9.jpg.Alphaware	Dropped File	23.82 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c13ec530e20be11c0817ce8168bbad9d50c4991cf0c6a16dcd0a5b1c78c4a108	c:\users\keecfmwgj\videos\zu2jiwj2ww\ermdlpgee_opr8.mp4.alphaware, C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\eRmdlpgeE_oPR8.mp4.Alphaware	Dropped File	18.47 KB	text/plain	Access, Create, Write	CLEAN
80d357e6a0e4ede25c9968015fb934c7c6f4f03f52977ff8c818aea55348fca5	C:\Users\kEecfMwgj\Desktop\fWyG0v4r7alxC.gif.Alphaware, c:\users\keecfmwgj\desktop\fwyg0v4r7aixc.gif.alphaware	Dropped File	127.41 KB	text/plain	Access, Create, Write	CLEAN
2d2abc33631ed95a36d5bafee9ce9b939f239066a175cdc709b91454d2abc654	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\jnmmi.ots.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\jNMMi.ots.lnk.Alphaware	Dropped File	904 bytes	text/plain	Access, Create, Write	CLEAN
0fbf57404767dcfd0358f8a951466de15157ed419efdd5075c105acd415bcfd6	C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\8lwQtag2z.swf.Alphaware, c:\users\keecfmwgj\videos\jvugc2sabzfj\8lwqtag2z.swf.alphaware	Dropped File	66.97 KB	text/plain	Access, Create, Write	CLEAN
ae1b9a2144b3d41bf9949dfe49300fe82c2392f1ca946e2a1750fe5dfa6c1ec9	C:\Users\kEecfMwgj\Documents\y-0\584vk2Slwl33KAWC.docx.Alphaware, c:\users\keecfmwgj\documents\y-0\584vk2slwl33kawc.docx.alphaware	Dropped File	133.13 KB	text/plain	Access, Create, Write	CLEAN
6f497dfe6f3ba6b1c64ea1add0bbdf59c74da2f4884ce2e39c6b3bf265417602	C:\Users\kEecfMwgj\Videos\ZShqFxkOqd6c5.mp4.Alphaware, c:\users\keecfmwgj\videos\zshqfxkoqd6c5.mp4.alphaware	Dropped File	118.43 KB	text/plain	Access, Create, Write	CLEAN
f58c27f51a897559e46a78b52fa65995f2f859e491177972c67573d3f8b59c67	c:\users\keecfmwgj\videos\jvugc2sabzfj\4_p930hvcz_\bpvw70tznos_6.avi.alphaware, C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\4_p930HVcZ_\BPvw70tznoS_6.avi.Alphaware	Dropped File	59.84 KB	text/plain	Access, Create, Write	CLEAN
f4516354344abd7f6c69b1f5537a976df05498d2ded74f1b2c677b5e7a22d875	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\qs1esam6mnjquw3k.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Qs1EsaM6mnJQuW3k.lnk.Alphaware	Dropped File	1.22 KB	text/plain	Access, Create, Write	CLEAN
901fe76d76119f8541e34eca25315dd22026a8fd5f68767eafd7a3b91c98190d	C:\Users\kEecfMwgj\Desktop\IPAZp7HIeyfBa.avi.Alphaware, c:\users\keecfmwgj\desktop\ipazp7hieyfba.avi.alphaware	Dropped File	121.53 KB	text/plain	Access, Create, Write	CLEAN
9aefa6a6f707c0eec0a66a26e9669338659e46f4c603a8f050dcce3691adbf6b	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\cgtmsh0_nmfpfsqohtip.lnk.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\CGtmsH0_nmfPfsQOHtip.lnk.Alphaware	Dropped File	3.43 KB	text/plain	Access, Create, Write	CLEAN
b53d357db181213db373b439f1192de02ceffddbc89fb2deb293b49c018fb18f	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\sendto\desktop.ini.alphaware, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini.Alphaware	Dropped File	948 bytes	text/plain	Access, Create, Write	CLEAN
2bb7672661a96f25db12a0588edf8b9c3f3fc01e1036a7c6c1889172edabcf56	C:\Users\kEecfMwgj\Links\OneDrive.lnk.Alphaware, c:\users\keecfmwgj\links\onedrive.lnk.alphaware	Dropped File	2.20 KB	text/plain	Access, Create, Write	CLEAN
1fef2c8f39b3a5e4ef5a9a9bb78f070e7e3b2f1c01370e69c72a60080c8e6618	c:\users\keecfmwgj\pictures\w0y6k3cxjraf-y2ue6\jo7fjz3qqw1.gif.alphaware, C:\Users\kEecfMwgj\Pictures\w0y6K3cxjraf-y2uE6\jo7Fjz3qQw1.gif.Alphaware	Dropped File	8.03 KB	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d14b3669cb670533eadfc1f8b07096a1277de39dd199c13810fbc1ce67e279b9	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\2cvjqDL8AbrH.lnk.Alphaware, c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\2cvjqdl8abrh.lnk.alphaware	Dropped File	1.47 KB	text/plain	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\tvhtwfsg.flv.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\1BM5_1HkTZyXvgJAFgc.flv.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\8wsZ\sRZM.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQlR\eUSZ\awU7DFoRrK67OUHE2Uat.mp4.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\internet explorer (64-bit).lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\SjIEHWNzBPbEPK.ppt.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\eRiABnWG9I.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\j99z9mopk.pdf.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\w0y6k3cxjraf-y2ue6.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\Recent\Templates.LNK.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\mxWMxpSlb1Z2y3xfhO0.swf.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\yqlr.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\AZ80w8eAVF6qLdtcVJl\zR 1JJINH15QPReboG.png.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\8wsZ\vGw-gK7bU.mp3.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\nqr9nqmjn0 i.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\8wsZ\VrH278.wav.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\internet explorer.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\public\music\sample music\maid with the flaxen hair.mp3.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\Recent\index.dat.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\atmirxtqukvsiqb.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\uk0_t4zjwac.wav.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Explorer.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\uklsvp0oeoluyu0aa\jc7ce.wav.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\sraa yna6fae6hy.m4a.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\shows desktop.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\8wsZ\7ucxK0MmIS9f.mp3.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\pydvqxrn.mkv.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\accessories\system tools\private character editor.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\accessories\accessibility\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\1yppaa.jpg.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\daw-ipdr7ovxj2g.docx.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\NQCf5ew.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\cgtmsh0_nmfpfsqohtip\vo9mo3eeu2 slpqjwfm.png.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\UKlsVP0OeoLUyu0aA.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\1tTeAH3Idl9j.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\4_p930HVcZ_\c4x.flv.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\ebght40n22e7ya.mp3.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\onedrive\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\administrative tools\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\maintenance\help.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Cookies\keecfmwgj@support.microsoft[3].txt.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\t2V3lQcrptDn.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\y-0\beaeacczbwdfqo39\2y7nvezda.ppt.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\5jdQ8S\rSuF1L1G3gyu.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\qs1esam6mnjquw3k.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\jvuGC2saBZF J\bC7JKZ.swf.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RkF0hT0Xfp-m3q.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\qq69aqvcd-_ggmfehfcj.pdf.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\jvugc2sabzf j\4_p930hvcz_\4iwuq2z09oquci.flv.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\ozdqhhdycahwn.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\mvpq.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\bnr8t.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\asl2thvdjfyifjk_mixu.wav.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\UKlsVP0OeoLUyu0aA\Kmo_0PpyMcbzk.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\0kv--h785b9BKHr7X8.mkv.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\t2oMmxPi.flv.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\584vk2Slwl33KAWC.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\gerlghj-j1fq.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\IoUNPPwfOO3o6JZNAZ0x.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\yyaadtzvoxxesxd.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\oopofnm9s\yyaadtzvoxxesxd.bmp.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\dz5o.docx.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\JPY6YvdnrHDp.mp3.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Duc5tpM3PDmAXr1.ots.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\nbyvlogs.m4a.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\pydvqxrn.mkv.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\dz5o.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\JtwiWA.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\RBnxFLdoe6j5FMDq\JlGdXo.wav.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\PPCDrQ5.docx.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\az80w8eavf6qldtcvji\r5baui uaurz 0kbpe.jpg.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\NqR9nQMJn0 l\H-iXHNw3Q.jpg.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\xfj_k_QyvZX0.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\OnrpsaEkvylzPJqZCM2l.mkv.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\9wzxgia1p9.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fPmhr.wav.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\sd_mf\e4w8io-jmf\az80w8eavf6qldtcvji\upx6uzdipr.gif.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\cgtmsh0_nmfpfsqohtip\zkwjy960tnphzx9r1d2d.jpg.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\vo9mo3eeu2 slpqjwfm.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\rkf0ht0xfp-m3q.pptx.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\d_cm4s7fp.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\q_m8XgrWIwVpa_ok Jpb.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\RBnxFLdoe6j5FMDq.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\accessories\accessibility\magnify.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\privacie\index.dat.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\d_cm4s7fp.pptx.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\zoe1ltkimcuaahrwbxf9.swf.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\rKqcydSq.mkv.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\kz1hatiactkd69pq32m.m4a.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\H-iXHNw3Q.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer (2).lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\w1qxuxltv5acd7eku7.mkv.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\5oehl_lcmalfb_z.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\jvxZB--pZ8D4tDAf.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\desktop.ini.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\8wsZ\q_JfZqnkZKS-.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\jnmmi.ots.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\t2V3lQcrptDn.rtf.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\start menu\programs\accessories\system tools\control panel.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\internet explorer\quick launch\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\QCDZICFDAJnNsJNJRg.m4a.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\miKlgwo4kuAJyz.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\0kv--h785b9bkhr7x8.mkv.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\public\pictures\sample pictures\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\CKk3Lv0r a.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\ZiOJla1 Q-SXSl2W5.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\zOe1LTkImCuAAhrwbXf9.swf.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\rbnxfldoe6j5fmdq\6osm8h3fxy3kmcyqkdk.m4a.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Run.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\rmPQA vuvasucn14.mkv.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\4a87c_8npb.pps.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\ozdqhhdycahwn.odp.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\8wsz.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\my pictures.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\v8u50bnoh.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player (2).lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\5jdq8s\zmtegoau5-f.wav.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\jvugc2sabzfj\4_p930hvcz_\bpvw70tznos_6.avi.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Links\Downloads.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\zu2jiwj2ww\tkqjzn.flv.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\GwoFAC.pdf.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Pictures\sD_Mf\e4W8iO-jmf\NqR9nQMJn0l\WsNjcAtuTT8n1nv.gif.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\vcnvmrhf2u7xxjbaxrmb.pps.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\zR1JJINH15QPReboG.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\T6C4G_g_0sfV1dVJsM.pptx.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\public\pictures\sample pictures\koala.jpg.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\zu2JIWj2WW\yQIR\FPYGUZhtS1g3J.mp4.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\5jdQ8S\rZ3-_8o.wav.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\JmY86mr.swf.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\jvugc2sabzf j\jlpj6j.flv.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\JhfS93kCXhB0dS47UXO.swf.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\1wWkN7zA3pJvJ0l2.pdf.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Links\desktop.ini.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\WQTdEEFonuZ7KxbDBX.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Recent\Z3ZXfX.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\pptfqfujeeheoaqm.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\cgtmsh0_nmfpfsqohtip\h8wehqdt-nllywl7w3.gif.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\e4w8io-jmf.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\y-0\beaeacczBwDfQo39\7Cu9qgyf.ods.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\desktop.ini.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\computer.lnk.Alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\recent\eusz.lnk.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\roaming\microsoft\bibliography\style\iso690nmerical.xsl.alphaware	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\Logging	access, read	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\Setup	access	wmiprvse.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress	access, read	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	access, create	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	alphaware.exe, svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\Log File Max Size	access, read	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	svchost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing	access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
svchost.exe	"C:\Users\kEecfMwgj\AppData\Roaming\svchost.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet & wmic shadowcopy delete	SUSPICIOUS
wmic.exe	wmic shadowcopy delete	SUSPICIOUS
alphaware.exe	"C:\Users\kEecfMwgj\Desktop\Alphaware.exe"	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	CLEAN
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no	CLEAN
bcdedit.exe	bcdedit /set {default} bootstatuspolicy ignoreallfailures	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /C wbadmin delete catalog -quiet	CLEAN
wbadmin.exe	wbadmin delete catalog -quiet	CLEAN
bcdedit.exe	bcdedit /set {default} recoveryenabled no	CLEAN
notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\kEecfMwgj\AppData\Roaming\readme.txt	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.2.0
Dynamic Engine Version	2023.2.0 / 04/13/2023 04:20
Static Engine Version	2023.2.0.0 / 2023-04-13 03:00:20
AV Exceptions Version	2023.2.1.4 / 2023-04-17 18:38:13
Link Detonation Heuristics Version	2023.2.1.8 / 2023-05-05 16:25:00
Smart Memory Dumping Rules Version	2023.2.1.4 / 2023-04-17 18:38:13
Config Extractors Version	2023.2.1.9 / 2023-05-12 15:33:54
Signature Trust Store Version	2023.2.1.4 / 2023-04-17 18:38:13
VMRay Threat Identifiers Version	2023.2.1.9 / 2023-05-12 15:33:54
YARA Built-in Ruleset Version	2023.2.1.9

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2023-05-18 05:32:09
Built-in AV Database Records	13632679

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop

Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows