MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Setup.exe**
ID	#9566692
MD5	da6b7ddd28dc387bcd10b180c9bdff58
SHA1	c29cd8c4370576afb63deea020bcafd8c0638de0
SHA256	077eee74b8f1227707b389a953234756d3bf8b78108a24f132bd5feb209dd8f6
File Size	12548.00 KB
Report Created	2023-12-27 00:56 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 21 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends new extensions to many filenames	1	Ransomware
	• Renames 133 files by appending the extension ".syrk".			
5/5	User Data Modification	Encrypts content of user files	1	Ransomware
	• (Process #9) powershell.exe encrypts the content of multiple user files.			
4/5	Defense Evasion	Bypasses Windows User Account Control (UAC)	1	-
	• (Process #1) setup.exe disables UAC dialog via registry.			
4/5	Reputation	Malicious file detected via reputation	3	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels file "C:\Users\Public\Documents\cgo46ea565sdfse7.exe" as Mal/Generic-S. • Reputation analysis labels file "C:\Users\Public\Documents\startSF.exe" as Mal/Generic-S.			
3/5	System Modification	Modifies system configuration	1	-
	• (Process #10) limeusb_csharp.exe disables the display of hidden files and folders.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #1) setup.exe sets the desktop wallpaper to the file "C:\51875.jpg".			
2/5	Hide Tracks	Hides files	4	-
	• (Process #1) setup.exe hides the file "C:\Users\Public\Documents\" by setting its "hidden" attribute. • (Process #1) setup.exe hides the file "C:\Users\Default\AppData\Local\Microsoft\-pw+.txt" by setting its "hidden" attribute. • (Process #1) setup.exe hides the file "C:\Users\Default\AppData\Local\Microsoft\+dp-.txt" by setting its "hidden" attribute. • (Process #1) setup.exe hides the file "C:\Users\Default\AppData\Local\Microsoft\-i+.txt" by setting its "hidden" attribute.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) setup.exe enables process privilege "SeDebugPrivilege".			
1/5	Input Capture	Monitors mouse movements and clicks	1	-
	• (Process #1) setup.exe frequently reads the state of a mouse button by API.			
1/5	Defense Evasion	Accesses volumes directly	1	-
	• (Process #9) powershell.exe opens a handle to directly access the volume "C".			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) setup.exe resolves hostname "gr9wgs94fg5sb3y8l.000webhostapp.com" to IP "145.14.144.29".			
1/5	Execution	Executes dropped PE file	3	-
	• Executes dropped file "C:\Users\Public\Documents\LimeUSB_Csharp.exe". • Executes dropped file "C:\Users\Public\Documents\cgo46ea565sdfse7.exe". • Executes dropped file "C:\Users\Public\Documents\startSF.exe".			

Score	Category	Operation	Count	Classification
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #9) powershell.exe creates an above average number of files.			
1/5	Obfuscation	The binary file was created with a packer	1	-
	• File "C:\Users\Public\Documents\startSF.exe" is packed with "PureBasic 4.x -> Neil Hodgson".			

Mitre ATT&CK Matrix

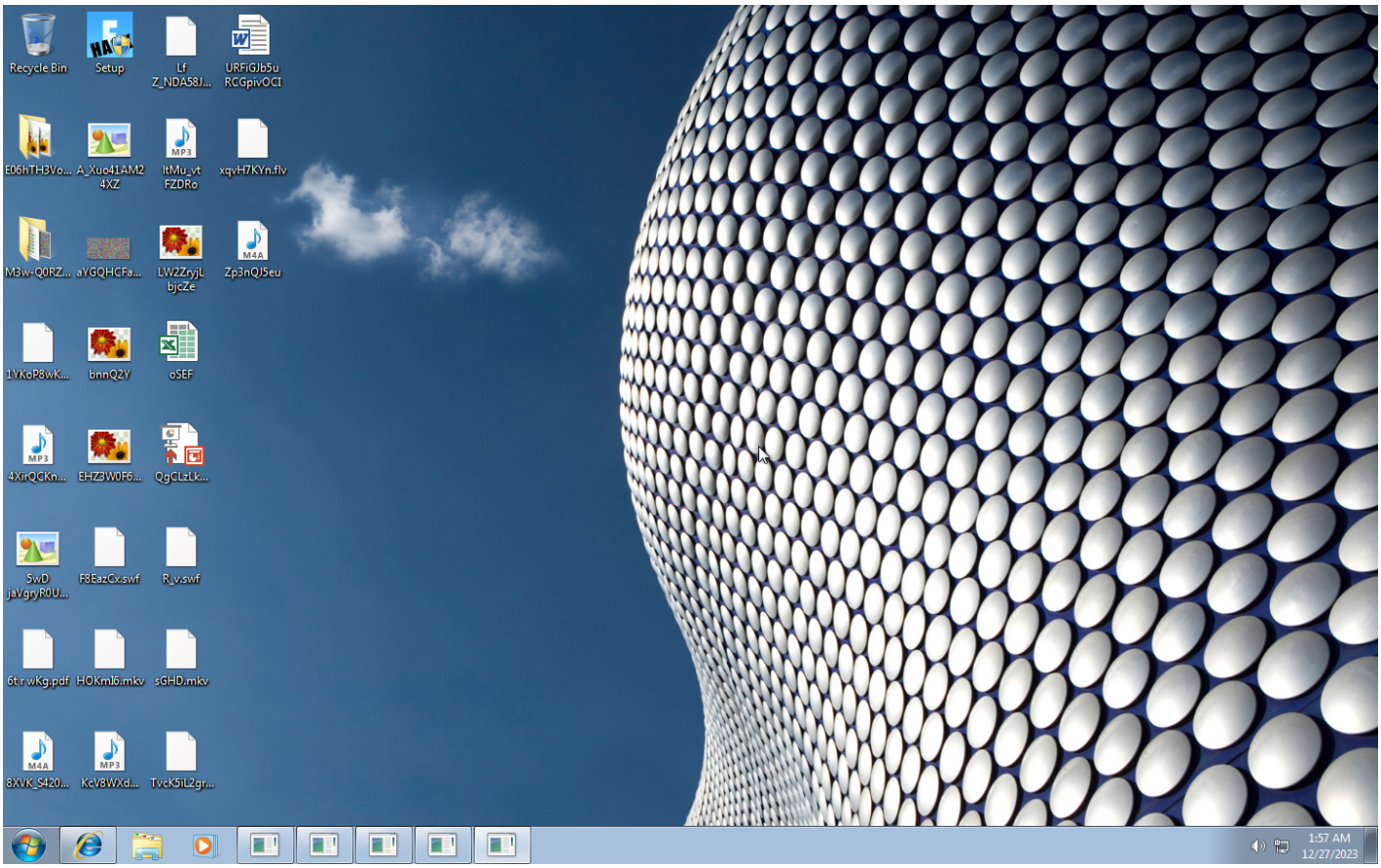
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1158 Hidden Files and Directories		#T1112 Modify Registry	#T1056 Input Capture			#T1056 Input Capture			#T1491 Defacement
				#T1158 Hidden Files and Directories							#T1486 Data Encrypted for Impact
				#T1006 File System Logical Offsets							
				#T1045 Software Packing							
				#T1027 Obfuscated Files or Information							

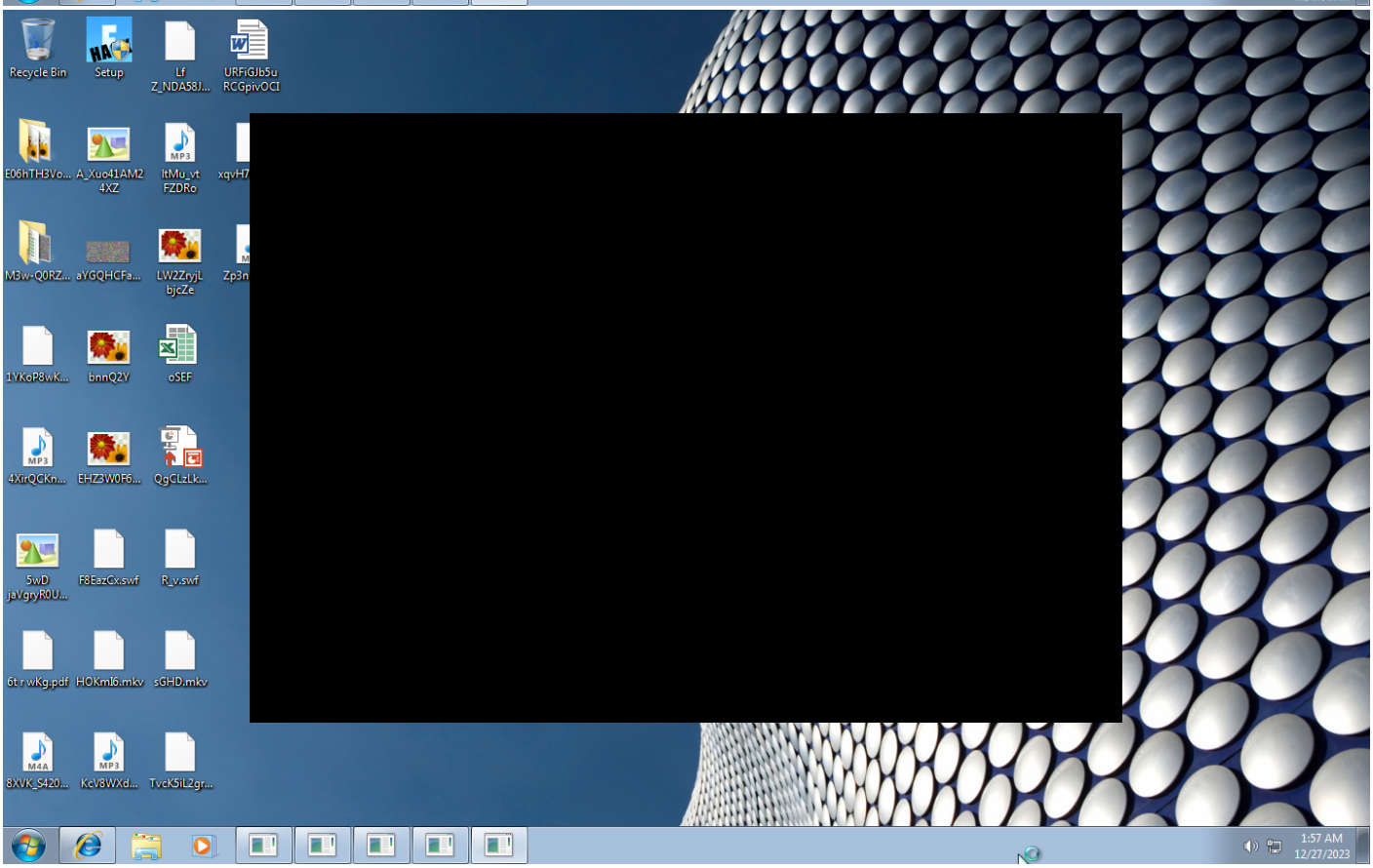
Sample Information

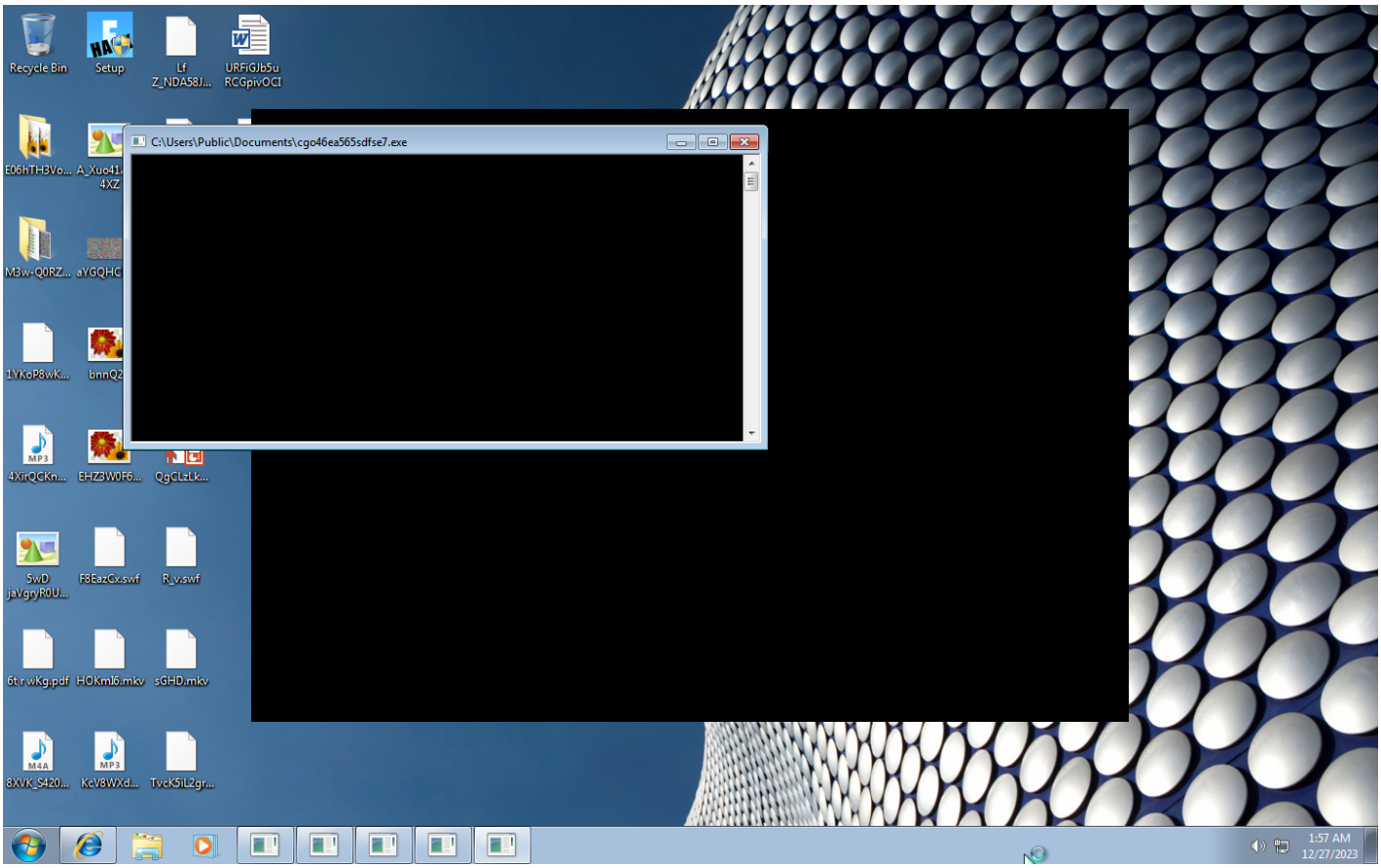
ID	#9566692
MD5	da6b7ddd28dc387bcd10b180c9bdff58
SHA1	c29cd8c4370576afb63deea020bcafd8c0638de0
SHA256	077eee74b8f1227707b389a953234756d3bf8b78108a24f132bd5feb209dd8f6
SSDeep	98304:79Xv0eg9Xv0WJEdbxAtwOT3vjONrdbxAtQGTgvjOmh9Xvp79XvTY9XvRy9Xvjo9V:tqiRJAUkotsOFdRvCkn
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	Setup.exe
File Size	12548.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

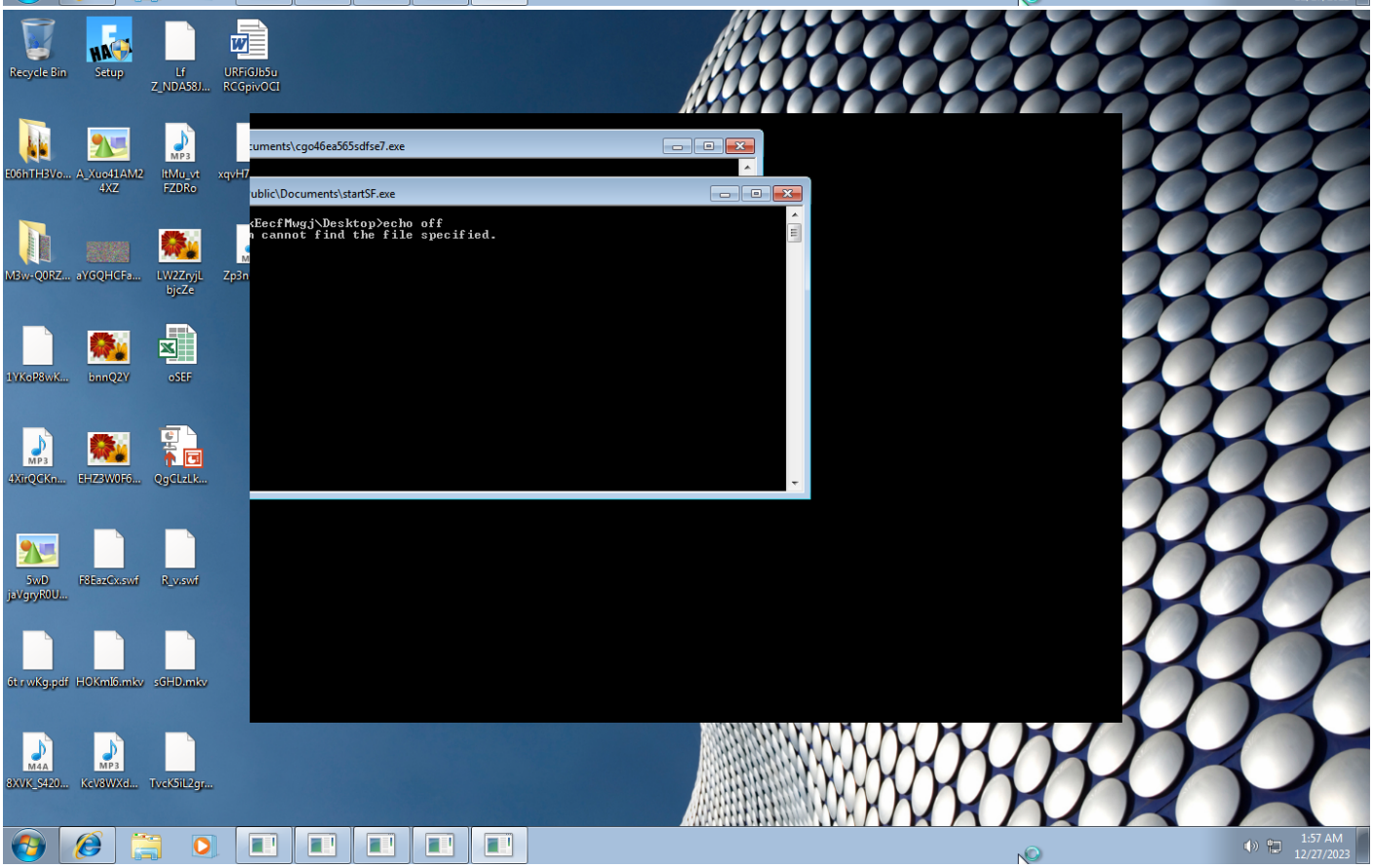
Analysis Information

Creation Time	2023-12-27 00:56 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	32
Execution Successful	True
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


Recycle Bin
Setup
Lf Z_NDA58J...
URFiGJb5u RCGpivOCI
E06hTH3Vo...
A_Xuo41AM2 4XZ
ltMu_vt FZDRo
xqvH7KYn.flv
M3w-Q0RZ...
aYGQHCFa...
LW2ZryjL bjcZe
Zp3nQJ5eu
1YKoP8wK...
bnnQ2Y
oSEF
4XirQCKn...
EHZ3W0F6...
QgCLzLk...
5wD jaVgryR0U...
F8EazCx.swf
R_v.swf
6t r wKg.pdf
HOKml6.mkv
sGHD.mkv
8XVK_S420...
KcV8WXd...
TvcK5iL2gr...
1:57 AM
12/27/2023


Recycle Bin
Setup
Lf Z_NDA58J...
URFiGJb5u RCGpivOCI
E06hTH3Vo...
A_Xuo41AM2 4XZ
ltMu_vt FZDRo
M3w-Q0RZ...
aYGQHCFa...
LW2ZryjL bjcZe
1YKoP8wK...
bnnQ2Y
oSEF
4XirQCKn...
EHZ3W0F6...
QgCLzLk...
5wD jaVgryR0U...
F8EazCx.swf
R_v.swf
6t r wKg.pdf
HOKml6.mkv
sGHD.mkv
8XVK_S420...
KcV8WXd...
TvcK5iL2gr...
1:57 AM
12/27/2023





Screenshots truncated

NETWORK

General

81 bytes total sent

147 bytes total received

1 ports 53

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

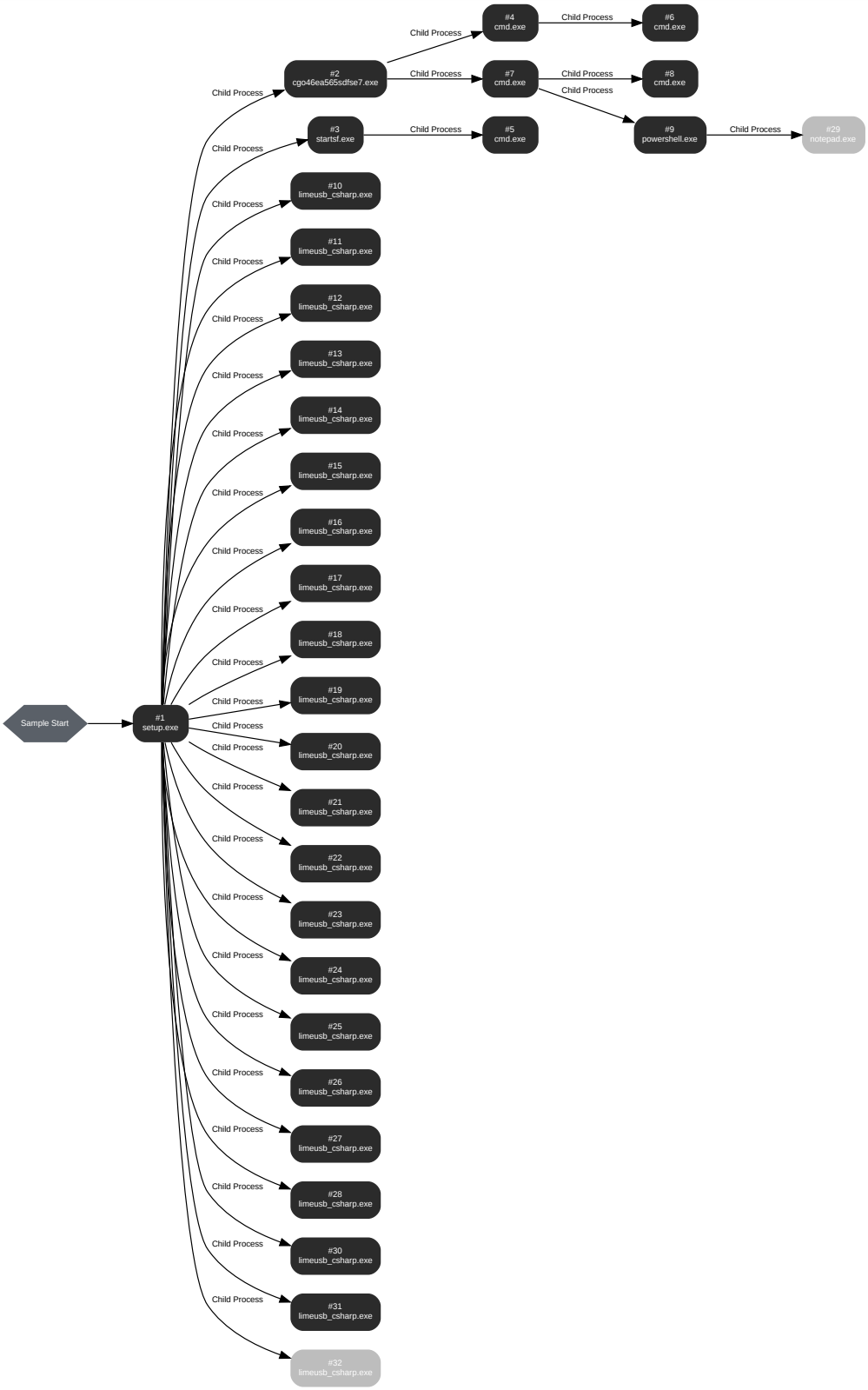
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	gr9wgs94fg5sb3y8l[.]000webhostapp[.]com, us-east-1[.]route-1[.]000webhost[.]awex[.]io	NO_ERROR	145.14.144.29	us-east-1[.]route-1[.]000webhost[.]awex[.]io	CLEAN

BEHAVIOR

Process Graph



Process #1: setup.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\setup.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\Setup.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 43609, Reason: Analysis Target
Unmonitor End Time	End Time: 288780, Reason: Terminated by timeout
Monitor duration	245.17s
Return Code	Unknown
PID	2356
Parent PID	2020
Bitness	32 Bit

Dropped Files (8)

File Name	File Size	SHA256	YARA Match
C:\Users\Default\AppData\Local\Microsoft\-pw+.txt	31 bytes	ba89a9d2bcd68421d979cce7880013eef84ce7bf5fb7d4f095719334a28defa6	✖
-	8.03 KB	2be64981c880589971a44f69e41bd016120f06a6475e3ba3aed629edeaecc8a9	✖
C:\Users\Public\Documents\LimeUSB_Csharp.exe	10240.00 KB	2e137c252a41187d2e70e2a8066d93268a95cb54b0b7a38feed7fa8c3c7b0de2	✖
-	108.52 KB	cb4e2511e5a723b966e80a5ec8c465f7337b003f19c308697cf98a5b36ae71c8	✖
C:\Users\Public\Documents\cgo46ea565sdfse7.exe	349.07 KB	c239d501439b776e93085925eb132ff164b1f3ba4fdc356a00045e8674dc1387	✖
C:\Users\Default\AppData\Local\Microsoft\+dp-.txt	64 bytes	54d1ffe932df5cddabe81236dedb09062af18ff956d8f60afd67f6282b094a66	✖
C:\Users\Default\AppData\Local\Microsoft\-i+.txt	26 bytes	6d8a951f265ef56f25b2341322d3fc205af4a914da83880fa45a263213d5ed69	✖
C:\Users\Public\Documents\startSF.exe	89.00 KB	31c3e1c03b15347bf8184854e65261a81ba12db0dcf3aeb5344ced6d8321ddf1	✖

Host Behavior

Type	Count
Registry	1322
File	309
Module	65
Window	181
System	7497
-	1
-	1
Process	24
Keyboard	5071
User	1

Network Behavior

Type	Count
DNS	1

Process #2: cgo46ea565sdfse7.exe

ID	2
File Name	c:\users\public\documents\cgo46ea565sdfse7.exe
Command Line	"C:\Users\Public\Documents\cgo46ea565sdfse7.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 61126, Reason: Child Process
Unmonitor End Time	End Time: 266923, Reason: Terminated
Monitor duration	205.80s
Return Code	0
PID	2412
Parent PID	2356
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Process	2

Process #3: startsf.exe

ID	3
File Name	c:\users\public\documents\startsf.exe
Command Line	"C:\Users\Public\Documents\startSF.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 61364, Reason: Child Process
Unmonitor End Time	End Time: 63708, Reason: Terminated
Monitor duration	2.34s
Return Code	1
PID	2432
Parent PID	2356
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.bat	159 bytes	1f5900bf3f1044b0469612875a23c6f8d3569608ac1ee27ed77fcbc0131dbdfe	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	17
File	19
System	34
Process	2
Environment	1

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c cmd.exe /c mkdir %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher & cd %USERPROFILE%\Docume... ...nmail.com to recover them.' ^> $home\Desktop\Readme_now.txt >> cry.ps1 & echo start $home\Desktop\Readme_now.txt >> cry.ps1 & exit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 61676, Reason: Child Process
Unmonitor End Time	End Time: 64772, Reason: Terminated
Monitor duration	3.10s
Return Code	0
PID	2460
Parent PID	2412
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1	692 bytes	2a57109b5ba1058449ab54984eda14294d760a252a0af44af3d37270dc1ad0ad	✖
Cipher.psm1	5.23 KB	05cbcd057e2b47ddaf0b74ddf01b86ebd9b9ecbaa5cc66f8f9fdf02cd22e017d	✖

Host Behavior

Type	Count
Module	1
Environment	12
File	1310
Process	2

Process #5: cmd.exe

ID	5
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\sysnative\cmd" /c "C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.bat C:\Users\Public\Documents\startSF.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62221, Reason: Child Process
Unmonitor End Time	End Time: 63574, Reason: Terminated
Monitor duration	1.35s
Return Code	1
PID	2472
Parent PID	2432
Bitness	64 Bit

Host Behavior

Type	Count
Module	5
Environment	3
File	86

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c mkdir C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62656, Reason: Child Process
Unmonitor End Time	End Time: 63856, Reason: Terminated
Monitor duration	1.20s
Return Code	0
PID	2652
Parent PID	2460
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	10

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c cmd.exe /c cd %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher & echo Remove-Item -path $ho... ... \Cipher\cry.ps1 & powershell -ExecutionPolicy ByPass -File %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1 & exit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63765, Reason: Child Process
Unmonitor End Time	End Time: 266815, Reason: Terminated
Monitor duration	203.05s
Return Code	0
PID	1304
Parent PID	2412
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	19
File	35
Process	2

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd.exe /c cd C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64014, Reason: Child Process
Unmonitor End Time	End Time: 65302, Reason: Terminated
Monitor duration	1.29s
Return Code	0
PID	1484
Parent PID	1304
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	11
Process	1
Environment	2

Process #9: powershell.exe

ID	9
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	powershell -ExecutionPolicy ByPass -File C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64399, Reason: Child Process
Unmonitor End Time	End Time: 266815, Reason: Terminated
Monitor duration	202.42s
Return Code	0
PID	2476
Parent PID	1304
Bitness	32 Bit

Dropped Files (134)

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\t_ v5c6i.png.syrk	81.54 KB	654070e295114ae7dcd103d1898fb060b0d719e099b0110f0981eb4f479194e4	✖
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BtaCh0Rv1i6GNNdmI.png.Syrk	18.25 KB	9b1d46658d392bc49324587ab7f48ed7ebdab21aedf3e8edc1b84eb518258bb3	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ln8yfcu_yh0.wav.syrk	62.18 KB	09eca56ca95f5d48299d311ff5185519568f92ceadb9bff7086ce8436c7ceca2	✖
c:\users\keecfmwgj\pictures\2r7o-shzef3qr6zs_c.gif.syrk	11.74 KB	0088e1df8972886c8622e3d5f52f87f64e8c0db4c143a2c9161e44ea1cd25b0f	✖
c:\users\keecfmwgj\desktop\lw2zryjl bjcze.png.syrk	54.30 KB	f1f1aa7a30c1fcd85a7cbf7d228f98876cbc44e280e5b75fcf7dad9bb559c2e5	✖
c:\users\keecfmwgj\documents\gadgp30\qjecmq_e4_60ksbs_d7zx.pptx.syrk	14.14 KB	75275ef7e3aab964d0230a3818dcf3b17ee352a9b466b41b5d641a7fc856b141	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\ugb vvdin.pdf.syrk	42.72 KB	8a0de635eef6ae052bc93ea712423f362f8c6131f521656d929a85396c114488	✖
c:\users\keecfmwgj\documents\qdt8j-_xcq 65llcpzig.pptx.syrk	29.71 KB	24094bb37a0d069d23bda61d33474ba70e4378bd58d39994b64ffdbff858cada	✖
C:\Users\kEecfMwgj\Pictures\kwI_sPi1.png.Syrk	36.94 KB	77553e052f0a975911da42aedc8e0bf2196f346c820208d6391ec7d82a89b507	✖
c:\users\keecfmwgj\videos\gjgfz-.mp4.syrk	66.36 KB	24e509d3f3df4cb17ad3350892c541c59de7465df67406d4eef4ed3a5e46f2cb	✖
c:\users\keecfmwgj\desktop\ltmu_vt fzdro.mp3.syrk	49.66 KB	63a6b1e02d35d062e72ad252f605c7fba433d3cf7fb764155253461765bd06f2	✖
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\OUWK.mp3.Syrk	4.38 KB	42abece8b8374ec41a384407d5a12b116dc74d1f27fa597a49114f09dd248acf	✖
C:\Users\kEecfMwgj\Documents\tcbu3AshPzFcR2r8Ck o.docx.Syrk	57.30 KB	1279fd3acd75d1e5c6b29b4df9c001c72c581eb9cfba8d440267ceb269a79bd0	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n7u6-hdfzcmk12ax.ppt.syrk	5.25 KB	d69461131d88a15fbf64eba37702c8017c52f10066f2e7dc9fb431565c405101	✖
C:\Users\kEecfMwgj\Pictures\6ZfnhezHZzwofrnONF.jpg.Syrk	67.14 KB	172c950dbc41bf6ea2870227cbaad003646c259b27a022b63d67e42fcbf3f014	✖
c:\users\keecfmwgj\pictures\8czrpcyd_m6g307p3uxk.png.syrk	78.30 KB	a82ce3b9110193471f62f7e8aafb9799d7125a47ebe94bc71999986d32ace1eb	✖
C:\Users\kEecfMwgj\Documents\yl14C.docx.Syrk	14.72 KB	c437d04f871e6424c828969fdeec8aa4509e5c6063f0c26478bf9d26c8f878a7	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\5wD jaVgryR0UBy6Yy26.gif.Syrk	50.55 KB	052c65ca957bcd04a26e04fe04d7dd538943060343aebcb3d21d8595baa22223	✖
C:\Users\kEecfMwgj\Pictures\8DVbrPzwsfunn.jpg.Syrk	51.33 KB	58a064d5257e3f2e145c09c0396e6c3413c9c1717659303b96ba85e879a690e6	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\hd6yww0khas8.ppt.syrk	51.27 KB	88b384a438a14086bfd3c7972cce6038c5f51a034973841fdc93f8a7a4894ce9	✖
C:\Users\kEecfMwgj\Documents\hQwa.pptx.Syrk	91.99 KB	b94515d82ce9a82f4e67ce1f32cb50d12a579e9266dd9c84eeb042154696161c	✖
c:\users\keecfmwgj\music\omcoseo.wav.syrk	99.55 KB	596ed2ba26fc25b1ebe3108ae2ffd8fccd23024b2a0426b06008f8fd849d70a3	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\O5Kq9mR4CC\ZDzv.mp3.Syrk	61.29 KB	bff18a4d12dc95648349c4c44c433a5883fb4685d31b393dae5ced79902db84d	✖
C:\Users\kEecfMwgj\Pictures\v30MfWJ0Z.jpg.Syrk	28.16 KB	2092b2bf529afcefc0eae35505ece1403ac3c783d59700d4d1399d512d671f1a	✖
c:\users\keecfmwgj\videos\ulsd6hewxcm_chkzb.avi.syrk	44.44 KB	365f0ae6285dc9f0d469e51f458e33ce2702ed53fe4b6f3230f06275045b08ba	✖
C:\Users\kEecfMwgj\Documents\zVu_x.xlsx.Syrk	49.85 KB	2702f45ec0f378dd4ee634a4d4a700e87b71ac90ad56649cce14084d85e81215	✖
c:\users\keecfmwgj\pictures\y a649h.jpg.syrk	24.71 KB	9a890251708b8caabb2ec2e4f53df7cc47723210161 81f2f1ea658f74231551d	✖
c:\users\keecfmwgj\documents\kzkisarpnjyn.xlsx.syrk	44.58 KB	030ff19c62a6127b358e8a9462509a3bf6a4306dc1fb5c3a9dd44cfe87d2a2f4	✖
C:\Users\kEecfMwgj\Pictures\CRAGPLrxjBWjbAs_pS.jpg.Syrk	6.25 KB	4344ca461620c066747fe78180686ffa952030ee43584cc4a9d897c5374191f4	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\appn7n4hto.pdf.syrk	40.33 KB	36450c6d7ff601cd6543fb38a6eecb0bb069063df3276d16038ba322d56c3f0e	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\O5Kq9mR4CC\n8siGXFTdMtKcZh\YBZFeG9.wav.Syrk	2.88 KB	7f7296bab0b7169ea969fa7e8b0fcd6fcc43eb3151a6b854656054cd2b253733	✖
c:\users\keecfmwgj\pictures\qjmibj2csojvn7un2o.bmp.syrk	37.07 KB	4190bc07768212b18635d98fe68ce1c1d5bf1e1ca19003b72039c460b757149f	✖
c:\users\keecfmwgj\pictures\uz- c.gif.syrk	62.24 KB	2ddac7b33946bf2158d4b6c543f5aaf860d4b32bac502fd58e6101c2ec6dc7b7	✖
c:\users\keecfmwgj\pictures\gn4io1vv8uthsx.png.syrk	31.29 KB	354508e4b82a4b0d81e45955855efd853ef2426a5035a7e715218e537a97ecfb	✖
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\x7ay0560rvhbasv7.bmp.syrk	55.58 KB	98ba79da92b6b14b87cb7a87ca80761780c5b4bde21143a7fe7ec552b262c8d9	✖
C:\Users\kEecfMwgj\Videos\TXd5XhbVM_gRmGa.mp4.Syrk	25.13 KB	5c5d16bed3ebf999377f7a62c8e3750efd043369cff963604e2ef4321a24c55c	✖
c:\users\keecfmwgj\pictures\1tp--jqrn7ickv.jpg.syrk	43.30 KB	1f3f4ecf25f0e7b023b9cd44c358e10d198f2307deb96c0feeadbf9ba04c0a31	✖
C:\Users\kEecfMwgj\Pictures\XOXL0s.gif.Syrk	75.82 KB	2dd901e5cc1444d7d97dadef2ab6ab852ec942b45009c6c82a0183510c69a912	✖
c:\users\keecfmwgj\videos\z8vxfzj-jnzgo.mp4.syrk	19.33 KB	039c8f3ed3deef27c1dfbdd3a54221a0650df6532290177eb3edc81b4e512f40	✖
C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\2NDvK0UV6C93Or2y33.xls.Syrk	49.00 KB	c40c4a1586e7838ad9a4c894c12173c08df382f53279931f20d3b4e09d0dc953	✖
C:\Users\kEecfMwgj\Documents\hiQyDV.pptx.Syrk	72.00 KB	3ed68bb573ec4d31ab8dd78169813d36cc0c3e9c88dbf6c4fba0a137cecf0a97	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\sb2jvq1jz7zixzf4.mp3.syrk	82.18 KB	1f7c93b5af11fa630b72a770b3f302dc531c9467ea6457b5cb41f5b3fbdebe06	✖
C:\Users\kEecfMwgj\Pictures\-20cBzLDzX_KXyz1k60.png.Syrk	40.49 KB	a5cdbcf0120cf4f97c13b0851956ff054b14f53b3517d5d19be090667df7fa6f	✖
c:\users\keecfmwgj\desktop\lf z_nda58jhfm.pdf.syrk	33.57 KB	78a0ed85c5f5dcd07142420b81df004eb51543322a6763dbc502f1e0980b7fea	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9 byo0\dP47.doc.Syrk	17.38 KB	c8d69816f228c5d92bcdef126b88f9f3f97ba0e92c999a96a4f7ef9c22667a94	✖
C:\Users\kEecfMwgj\Pictures\JhqgivuCmr9tbit.jpg.Syrk	59.04 KB	0fb0a7c611b7597d1b1f57b1d9433e05cc08f835100ca48babba4913dd43de1b	✖
c:\users\keecfmwgj\music\vazma_d1fuafei4nm_9.mp3.syrk	41.97 KB	055a52cf1872b7fa3dca042b79076567b8dd04821b79bc79696eb19b8ce505c5	✖
c:\users\keecfmwgj\music\zern8svva2_nmg.mp3.syrk	59.69 KB	51d39d6cf54ba294edc2e1648bb85351a78c167748d96618e0d526b64cf07fde	✖
c:\users\keecfmwgj\pictures\-yqu7r.jpg.syrk	96.85 KB	7659cb2d5739a47ee12cf6392c81822d5652712cb4d09761c2da4ede7770808f	✖
C:\Users\kEecfMwgj\Desktop\bnnQ2Y.png.Syrk	15.38 KB	6947b73d6cca5651f9134feb91dacf4b4080025f9cf3cc12e230d165ed28e3f6	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\xLkRw\MsuOsA4r0 23U.mp3.Syrk	52.49 KB	06a9abde69f3d19c6a15070f9dfd43d364a378550c8c5c7538408d0651289292	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\i82ix5otq989c-uh2jwl.mp3.syrk	74.29 KB	2cbb2137ef5b8aa3f0540394e797ecc21b5928e74edfb7faa5b50025641f1dd8	✖
c:\users\keecfmwgj\desktop\e06hth3voha0d\2 kc0zg1 rmrjok_gy.png.syrk	38.47 KB	f35548e3840816ab1f22fccfc5d519b051b321e22cba0f2351d6e47ffa365ac2	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\69v7zInse_6kw0ym e.mp3.syrk	10.41 KB	9e3742ea024c4b6a27ff7268b6f93acdd7686ab96f1da65d048bc05b3b72e84d	✖
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ncd4gg.jpg.syrk	97.44 KB	3214a38a14daecfea7d4f9030766aaa1aafc09e2f2dde2ae094f4ec09e908b6d	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\cptrf.ppt.syrk	65.04 KB	510ed9d07626dcee696852531b681fd35b0d812e2972c84b312085a9f6f39dcc	✖
c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\j_xc70wda-y.xlsx.syrk	38.52 KB	e61b085fc26e324f42ae1360489eeb321c23cf2411d613123b429f8068bb963b	✖
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\n2mooDz97hN Hy_Rw.doc.Syrk	25.18 KB	b44aae7dae20d884467694ee538427be6185cb745ecb213911fbf6fa9a4dc0ae	✖
C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\DgJ _YHDeXbtu1aaa9P7.pptx.Syrk	29.08 KB	d84f4d69d5bb1879cf13bd80d0b1be638db6ccf91b1550f70e1c5e6b77f93cd8	✖
C:\Users\kEecfMwgj\Pictures\mh_2oAjD6lQO.gif.Syrk	39.64 KB	5baaa1665fc5fcf36c9bce0a070a4083cc594e1a83cd5e3109e4a7c7dd9ba9ea	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\tjL0lG.mp3.Syrk	96.04 KB	0cea05e6120228dd58220ffb69a994b3d46b4aa2a40c64edd4400bc022557d05	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\jW54Ba8xSbY.wav.Syrk	10.30 KB	2ccb28df41fa02450046408495adc46b186989e5a02a6e356a1a332eb487e080	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\li_8a-uy.wav.syrk	40.50 KB	c01a20319d21070b2246e76ea0ea942882508c5f2603b40ff34eb1f6d2f52aa2	✖
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\JhXCNVX54s7.png.Syrk	15.21 KB	88231ddcf7f2bf245d626949b0d93dfe4d65367eab25e5ad474b087723d9de28	✖
C:\Users\kEecfMwgj\Music\M-QP9r3m\5q7ybWyiM4zx.wav.Syrk	4.18 KB	6aed588650635d21c3e6b3ed5845e2c3c6c373efa37fcc5519c486a5b0080b98	✖
c:\users\keecfmwgj\pictures\09ijundbva.gif.syrk	23.89 KB	eb0a5ab441858e6fc41007aa207d6501171706d969e24e1d321425a51991dc34	✖
C:\Users\kEecfMwgj\Pictures\dLcXhG3aWfBaiR.gif.Syrk	24.79 KB	9315c9391bf0c43e01475bccee8a530041d3d2626b7f8013abe32e4d58c68cce	✖
C:\Users\kEecfMwgj\Videos\YZQR06gE.avi.Syrk	79.35 KB	89d1489cc425cd1fde3a36222517150aa70d5278d9d20f0d95a5600c19aeb06e	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\xu9kprwq9.mp3.syrk	9.93 KB	9ab6a4c5ba3d6374398b51b1ca1f5904fde4cf58dafcb0dd23eb149f2c96df06	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\RE3_9X-yu-SSwhMc.mp3.Syrk	32.86 KB	450ed002f4b8c7f83e80c1e4976741808594d4d7cb523c304290af1e3bf19dbc	✖
c:\users\keecfmwgj\pictures\gm5d9kgelxbt.png.syrk	26.68 KB	e297a17c99bbed4c0963db8287a5ff390247d03a72a060ad0c04a2c523f5eab8	✖
C:\Users\kEecfMwgj\Pictures\ut5l85Hmrtdjra4F.jpg.Syrk	8.27 KB	49e1a97172dd5b92de31bee589c86752e112dfb3a3287fb4dde06c67e839b347	✖
c:\users\keecfmwgj\videos\xbhxbnsb3poh.mp4.syrk	91.02 KB	8652ba9110046eeebf36fec821690dbca5ab0cf701781fecff50adb651e13f74	✖
C:\Users\kEecfMwgj\Documents\tbolTOBf6oytAdVf.xls.Syrk	9.55 KB	276436b4dce497a38dca49137571beaa5824ef69f70cada037abfe9f77710a3e	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\mhccyt.docx.syrk	55.04 KB	7aeca36cc1c2a8fb03e8bd8c5786f2ca7b1bd2e2702e5371a54a10cb29597249	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\xlkrw\wwq2xl38e.mp3.syrk	91.39 KB	3964603d995993e318e5f473494c0ed085ead3029f8d46f6ea7c921810ef0d6e	✖
c:\users\keecfmwgj\desktop\e06hth3voha0d\4o6jjgbzavbwsb6-29.png.syrk	63.13 KB	bfaa0a4a07452c90befba1c0f1e22cc3cc2974222f66321725aa614e6417df7e	✖
C:\Users\kEecfMwgj\Pictures\gJalnSM9o_s.jpg.Syrk	13.96 KB	5516ef7b3486c11ef001d9013dc0f278a48975d59c85fb75f0688f897d84be6c	✖
c:\users\keecfmwgj\desktop\ehz3w0f6qpam.png.syrk	95.22 KB	61c6e143b3d888d07157b04c1fe42294e0c57c630cbd6eeaa7cb2026a0cb48f3	✖
c:\users\keecfmwgj\videos\wctn_hgh2xhblipzt0o.avi.syrk	7.18 KB	10663e99ff5e295979fe779f776bbc53b07896be38d142ba39d5b64fb3636047	✖
c:\users\keecfmwgj\pictures\tfnlk 0smrt1_1xww.gif.syrk	29.36 KB	49d147b5cdc9df105c880b372f8dbc18458d7585026d3e749528132e1ccd524c	✖
c:\users\keecfmwgj\pictures\bimh.png.syrk	41.89 KB	3ed81e36b36c1dfded79352d4f5d84cd453c6b1fd9fffdcccc3c08edf50664d9	✖
c:\users\keecfmwgj\pictures\neejrl4diryjsv.bmp.syrk	12.27 KB	05f38573d14f446971064b7c2532d797739fefbfe7489b6fbf4225f019df8abc	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\u0af.mp3.syrk	76.52 KB	303c93e49ed05431382581da782e6299bae015e341293a7a0c1a322f3b9b84b8	✖
c:\users\keecfmwgj\videos\xleaz.mp4.syrk	49.14 KB	7e5c0a4b50179f0ae93ad46813441b2e55fdb59b6bd5eddbd450c21aa485ee28	✖
c:\users\keecfmwgj\pictures\3r8d3dnv_alj.jpg.syrk	46.27 KB	7f7a7fe5d43430c7825ffed2f3662fc2ef5b9cd60ebe46de6e7cf1251a44cfea	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbufn\2-hxc4lfdhsq_mkvo.mp3.syrk	19.10 KB	78b6fba081d323bf751f2406e692527359e3cc4506dc2595b88e01c0ee4acf5b	✖
C:\Users\kEecfMwgj\Desktop\KcV8WXd6gM.mp3.Syrk	83.24 KB	e574cd45c1530de4846b48ec68ccdf6d8f15a9d2458368575eebbd7bc79db7b7	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\-hsXLHPSE2Gpg.mp3.Syrk	72.07 KB	c6f41b3640d0ab7e302136137e890e33f53b1efe65554e0a3f207c5d008d0840	✖
c:\users\keecfmwgj\desktop\e06hth3voha0d\5ifudwany.bmp.syrk	49.57 KB	dc838a4bdbc84dadab25864895e197ead4caf94974c41350561ac2a223e613a0	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\UOrn1.mp3.Syrk	61.72 KB	525f3ccaa8a1da2f6fb0e2f000db446e903fd7c5c29c15d84420f867127eee15	✖
c:\users\keecfmwgj\desktop\6t r wkg.pdf.syrk	44.71 KB	bdddeb9d0c3b9b89cb2fbb3137a5f7fc617bf13cadca1d193f1a7502202cf078	✖
C:\Users\kEecfMwgj\Documents\UYWqtSLk mI.docx.Syrk	80.25 KB	42a99a78bf3011643889b6396a91de639f69a5ec963eb3ff76b7627a1397b6ca	✖
C:\Users\kEecfMwgj\Pictures\qNxgBCMJFfZZ 6.bmp.Syrk	17.63 KB	c865cb57a3d943ed2135b8e0e790bfbaf0a67d75ec0eb38f0d92374094a5b3a2	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\waroxvlp.wav.syrk	37.11 KB	223f420922a8990ff59b429b0c90c35a811512649a3ce3972599e16e52bbd467	✖
C:\Users\kEecfMwgj\Documents\63C2JNBupUJaLCzjj.xlsx.Syrk	82.22 KB	abeb0eb440730f8fb3e4d815710bf52c0476b7b1709a6795e8c8f08aa293add5	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\Readme_now.txt	234 bytes	dca72b1d0a3327a56de391757ba37e384359876ac3d1e3d3c10f2e8f8b4b2d1d	✖
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9 byo0\JGqHA5Ln0.ppt.Syrk	97.18 KB	b39e335595b51ec09e2a5c150bc968880c31079d2d2bc2afef1ac9a60a872644	✖
C:\Users\kEecfMwgj\Pictures\LxEyCMb3cz G.png.Syrk	94.74 KB	d5f92769e115d0d64574d5cee2e7d44b96d01bde5ac2525de988c09de5541283	✖
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\TiksC6kLaNE3N.ppt.Syrk	51.71 KB	4d7694c5c927a5da321708a7bd50f069032af0e66d36f6e0293f551a6dfe2d02	✖
C:\Users\kEecfMwgj\Desktop\4XirQCKnN-C5.mp3.Syrk	61.39 KB	ec188048930cc6cfd159cf00434a08653db076c0a3228c62e3814cd9c576a10b	✖
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\vztlNW.docx.Syrk	90.49 KB	f482f765f278721fd2ca01a99d93bbeae83f8f879dd7971207fb0afef3e6cf23	✖
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BRmtCoyPLlLg.jpg.Syrk	1.80 KB	03863fc164d35e106d1445e224f6222348204961b1f6081117a390079330811e	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\0cA5darpWBXR.wav.Syrk	56.83 KB	888f7edb6bf699754e29071bfc6167075ff6fc2d67ad8dedbdc974bc87696a23	✖
C:\Users\kEecfMwgj\Desktop\aYGQHCFaIP7ms.bmp.Syrk	35.61 KB	95c750156132a986aa4168864e150db452ff15c579a83f959f72871795c12b6f	✖
c:\users\keecfmwgj\documents\0m2lwa6w2.docx.syrk	87.30 KB	ce69344077a84dcc4ba6f96737b7f1fa77c19b00c0f201ee76b3046ccd295ff5	✖
c:\users\keecfmwgj\documents\bx_hg08 qccc73wa.pptx.syrk	64.44 KB	7c15b7aed4be5d19e36536841e39e0e3a8538ec0cce3842c05f32e3d7fb6c952	✖
c:\users\keecfmwgj\videos\qpxgrgh9_6h.avi.syrk	64.29 KB	ccf26473d57d5e41910278dba046e038ac7fa80fa2975514d2b8db837ab9c20b	✖
c:\users\keecfmwgj\music\m9te.wav.syrk	24.47 KB	04d5e5f770e50d6961941f77bb31c5b9e7b2e8c33a17df9639c8553224b7881f	✖
C:\Users\kEecfMwgj\Documents\p9eQVmM.pptx.Syrk	61.68 KB	8c16c1c0f353de3ec419054467c27dc78a96fa47464654e210bf24032373e553	✖
c:\users\keecfmwgj\videos\h1j7hblziw7l.avi.syrk	19.32 KB	85e271c0eda333f5c00242ec7482cd2125cf59e31ac6966ac57f83a8260fbf31	✖
c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\eq95xs_2bmkwbb6.xls.syrk	56.10 KB	db8fc48228dcf7032bf37633c20f3a1526333725f316e0e2b55ca3d19bf597e4	✖
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n_go2uxegr7yuru5exh\nfwtjiionnnx.ppt.syrk	8.64 KB	677e6de07df80a6649d4974f22ac2dc9a0c0121e73420941275bcd91f2f306ac	✖
C:\Users\kEecfMwgj\Desktop\oSEF.xls.Syrk	67.66 KB	c7ed925dd319a9c92df829ec65f1354d236d4de40e6b6f8ae52a61522fae8542	✖
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ztjhwwr6z7cu6mtrpn.jpg.syrk	21.43 KB	c859e8900eae6214d6c8a94f517d9cfb141e587024201aec72ebe8c006b0688e	✖
C:\Users\kEecfMwgj\Documents\zm9nla-NPD71l4thrEn.xls.Syrk	32.33 KB	fdafe882325a70e738d50a846df931722fd4e1c59f19b6851b401e7c22471b6a	✖
C:\Users\kEecfMwgj\Pictures\tBNEwownJMNLIH-.gif.Syrk	44.72 KB	6a004621590e48d14fc76093da6e81edeb39ae27342b8504284f9ebe091fc098	✖
C:\Users\kEecfMwgj\Pictures\rokbMHY7.bmp.Syrk	43.80 KB	1c5b84a5d5ce04fd6a066ee035ed2fe73ce4ccaf16e1ad55aa298256adb78c05	✖
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\XXq4gabRA0W.wav.Syrk	8.22 KB	f2146e1641dc3a7f78f39b7002ced47a9ba62502a1c92951f5f71bbffbc574fc	✖
c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\ck5hblc73yemq3tcjmx.mp3.syrk	61.38 KB	1feb2da75eeb8971848ef37b21accf49462acc15688735c8b9b216f7e7d11ee1	✖
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\l9ni.wav.syrk	67.18 KB	40319d1ce18c61ca89aee161b0690aa7321f60ed0499f36b3020fea8e3580f14	✖
C:\Users\kEecfMwgj\Pictures\hwQvkSY6qlajdf.jpg.Syrk	41.50 KB	a201b847758164f63c76bcae9584f04c01387aee3820073e66782596ae6dbc2a	✖
C:\Users\kEecfMwgj\Music\MT00azHNzYeUklUK7WLY.wav.Syrk	92.82 KB	40fef7c27c8142c89dc0a645de52f1a9be73228a4e187edb66191a161f98864b	✖

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\ie3k6n7c0_b gizgjbf-.png.syrk	45.43 KB	9f048704fbaac9839cc4b459954c1eca325431f89738c5e65332d7090485a8ab	✖
C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\cDzt.ppt.Syrk	21.22 KB	538ccda2d98e4b68f7b265316b72faf7237ceb535335f895447e9ebedaea4f24	✖
C:\Users\kEecfMwgj\Desktop\A_Xuo41AM2 4XZ.gif.Syrk	66.57 KB	66447789876605798341 52e38b558fd54eb2c5931343139444713e9d955352fa	✖
c:\users\keecfmwgj\documents\a_x_tiv5stl.docx.syrk	2.85 KB	2928485fd3c9ef5962e3568e8237ec98bbac8740e91ee4508617c465166d0535	✖
C:\Users\kEecfMwgj\Pictures\-IvNIIwLh6qJBQ7x.bmp.Syrk	50.11 KB	03a92cee666c6930caceaaa407ce399e75d242c0d628fddfa16582870a0ee4fa	✖
C:\Users\kEecfMwgj\Documents\da4Yt5-_HXX-4.xlsx.Syrk	77.57 KB	30511e6572938110ef97c82fcfe6fc07d8d3e24b6ef1dd99af4b841e5f0921c7	✖
C:\Users\kEecfMwgj\Videos\qgeTWMdHrM.mp4.Syrk	81.52 KB	836eb1d2d7b9d1e283807b30246dca0ee2298dfe42274df44b50eacd1d9ef812	✖
C:\Users\kEecfMwgj\Documents\kLxyk2vrts2_ylshyl.xlsx.Syrk	58.13 KB	b80401295bdac40e332fa7acd778d47b0ae3ca56f2840c236a06d2b4d960d8c9	✖
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\-8f.xls.syrk	60.11 KB	ccd0b348a27958b4ea555a2ad7def37ba0c66ac96efde1022da0e6482c946bdb	✖
C:\Users\kEecfMwgj\Pictures\F-RYQ.jpg.Syrk	34.27 KB	2489cd2c6a01050aaac1f6cba713f712d6f6efd5583304c09c76e6383a430bbf	✖
c:\users\keecfmwgj\videos\zhli4r.mp4.syrk	1.61 KB	57fcc7081a456cfee4e3e0752d88f3d18e2fd82b76186f70e76829ca2b3dbf6b	✖

Host Behavior

Type	Count
Environment	2040
File	5831
System	52
Registry	88
Module	4
-	38
-	133
Process	1

Process #10: limeusb_csharp.exe

ID	10
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 73114, Reason: Child Process
Unmonitor End Time	End Time: 109981, Reason: Terminated
Monitor duration	36.87s
Return Code	0
PID	2680
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #11: limeusb_csharp.exe

ID	11
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82387, Reason: Child Process
Unmonitor End Time	End Time: 109953, Reason: Terminated
Monitor duration	27.57s
Return Code	0
PID	2580
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #12: limeusb_csharp.exe

ID	12
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92382, Reason: Child Process
Unmonitor End Time	End Time: 111244, Reason: Terminated
Monitor duration	18.86s
Return Code	0
PID	1524
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #13: limeusb_csharp.exe

ID	13
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 102731, Reason: Child Process
Unmonitor End Time	End Time: 116424, Reason: Terminated
Monitor duration	13.69s
Return Code	0
PID	2296
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #14: limeusb_csharp.exe

ID	14
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 113180, Reason: Child Process
Unmonitor End Time	End Time: 121244, Reason: Terminated
Monitor duration	8.06s
Return Code	0
PID	2332
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #15: limeusb_csharp.exe

ID	15
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 123215, Reason: Child Process
Unmonitor End Time	End Time: 133177, Reason: Terminated
Monitor duration	9.96s
Return Code	0
PID	2468
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #16: limeusb_csharp.exe

ID	16
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133539, Reason: Child Process
Unmonitor End Time	End Time: 144188, Reason: Terminated
Monitor duration	10.65s
Return Code	0
PID	924
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #17: limeusb_csharp.exe

ID	17
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143980, Reason: Child Process
Unmonitor End Time	End Time: 151910, Reason: Terminated
Monitor duration	7.93s
Return Code	0
PID	1960
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #18: limeusb_csharp.exe

ID	18
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 154374, Reason: Child Process
Unmonitor End Time	End Time: 160300, Reason: Terminated
Monitor duration	5.93s
Return Code	0
PID	2076
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #19: limeusb_csharp.exe

ID	19
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 164545, Reason: Child Process
Unmonitor End Time	End Time: 171341, Reason: Terminated
Monitor duration	6.80s
Return Code	0
PID	2544
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #20: limeusb_csharp.exe

ID	20
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 174730, Reason: Child Process
Unmonitor End Time	End Time: 182545, Reason: Terminated
Monitor duration	7.82s
Return Code	0
PID	1540
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #21: limeusb_csharp.exe

ID	21
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 185085, Reason: Child Process
Unmonitor End Time	End Time: 196197, Reason: Terminated
Monitor duration	11.11s
Return Code	0
PID	540
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #22: limeusb_csharp.exe

ID	22
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 195951, Reason: Child Process
Unmonitor End Time	End Time: 212559, Reason: Terminated
Monitor duration	16.61s
Return Code	0
PID	1528
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #23: limeusb_csharp.exe

ID	23
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 205757, Reason: Child Process
Unmonitor End Time	End Time: 221895, Reason: Terminated
Monitor duration	16.14s
Return Code	0
PID	2460
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #24: limeusb_csharp.exe

ID	24
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 217518, Reason: Child Process
Unmonitor End Time	End Time: 231145, Reason: Terminated
Monitor duration	13.63s
Return Code	0
PID	280
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #25: limeusb_csharp.exe

ID	25
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 226478, Reason: Child Process
Unmonitor End Time	End Time: 236340, Reason: Terminated
Monitor duration	9.86s
Return Code	0
PID	1064
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #26: limeusb_csharp.exe

ID	26
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 236860, Reason: Child Process
Unmonitor End Time	End Time: 243592, Reason: Terminated
Monitor duration	6.73s
Return Code	0
PID	1424
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #27: limeusb_csharp.exe

ID	27
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 247151, Reason: Child Process
Unmonitor End Time	End Time: 255803, Reason: Terminated
Monitor duration	8.65s
Return Code	0
PID	1960
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #28: limeusb_csharp.exe

ID	28
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 257317, Reason: Child Process
Unmonitor End Time	End Time: 263474, Reason: Terminated
Monitor duration	6.16s
Return Code	0
PID	1296
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #29: notepad.exe

ID	29
File Name	c:\windows\syswow64\notepad.exe
Command Line	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\kEecfMwgj\Desktop\Readme_now.txt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 263492, Reason: Child Process
Unmonitor End Time	End Time: 288780, Reason: Terminated by timeout
Monitor duration	25.29s
Return Code	Unknown
PID	1484
Parent PID	2476
Bitness	32 Bit

Process #30: limeusb_csharp.exe

ID	30
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 267506, Reason: Child Process
Unmonitor End Time	End Time: 272038, Reason: Terminated
Monitor duration	4.53s
Return Code	0
PID	2304
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #31: limeusb_csharp.exe

ID	31
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 277692, Reason: Child Process
Unmonitor End Time	End Time: 281884, Reason: Terminated
Monitor duration	4.19s
Return Code	0
PID	2620
Parent PID	2356
Bitness	64 Bit

Host Behavior

Type	Count
Registry	10

Process #32: limeusb_csharp.exe

ID	32
File Name	c:\users\public\documents\limeusb_csharp.exe
Command Line	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 287988, Reason: Child Process
Unmonitor End Time	End Time: 288780, Reason: Terminated by timeout
Monitor duration	0.79s
Return Code	Unknown
PID	1312
Parent PID	2356
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
077eee74b8f1227707b389a953234756d3bf8b78108a24f132bd5feb209dd8f6	C:\Users\kEecfMwgj\Desktop\Setup.exe	Sample File	12548.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
c239d501439b776e93085925eb132ff164b1f3ba4fdc356a00045e8674dc1387	C:\Users\Public\Documents\cgo46ea565sdfse7.exe	Dropped File	349.07 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
31c3e1c03b15347bf8184854e65261a81ba12db0dcf3aeb5344ced6d8321ddf1	C:\Users\Public\Documents\startSF.exe	Dropped File	89.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
2e137c252a41187d2e70e2a8066d93268a95cb54b0b7a38feed7fa8c3c7b0de2	C:\Users\Public\Documents\LimeUSB_Csharp.exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
aff8cb711b2b7e38bd15a3620a0c873727c0140afb26ca8959ff2a4b77ecc2c2	-	Extracted File	28.33 KB	image/png	-	CLEAN
2be64981c880589971a44f69e41bd016120f06a6475e3ba3aed629edeaecc8a9	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
cb4e2511e5a723b966e80a5ec8c465f7337b003f19c308697cf98a5b36ae71c8	c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	108.52 KB	application/octet-stream	-	CLEAN
1f5900bf3f1044b0469612875a23c6f8d3569608ac1ee27ed77fcbc0131dbdfe	C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.bat	Dropped File	159 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
05cbcd057e2b47ddaf0b74ddf01b86ebd9b9ecbaa5cc66f8f9fdf02cd22e017d	Cipher.psm1, C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\Cipher.psm1	Dropped File	5.23 KB	text/plain	Access, Create, Delete, Read, Write	CLEAN
2a57109b5ba1058449ab54984eda14294d760a252a0af44af3d37270dc1ad0ad	C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1, cry.ps1	Dropped File	692 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
ba89a9d2bcd68421d979cce7880013eef84ce7bf5fb7d4f095719334a28defa6	C:\Users\Default\AppData\Local\Microsoft\-pw+.txt	Dropped File	31 bytes	text/plain	Access, Create, Write	CLEAN
54d1ffe932df5cddabe81236dedb09062af18ff956d8f60afd67f6282b094a66	C:\Users\Default\AppData\Local\Microsoft\+dp-.txt	Dropped File	64 bytes	text/plain	Access, Create, Write	CLEAN
6d8a951f265ef56f25b2341322d3fc205af4a914da83880fa45a263213d5ed69	C:\Users\Default\AppData\Local\Microsoft\-i+.txt	Dropped File	26 bytes	text/plain	Access, Create, Write	CLEAN
1feb2da75eeb8971848ef37b21accf49462acc15688735c8b9b216f7e7d11ee1	c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\ck5hblc73yemq3tcjmx.mp3.syrk, C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\hfTktiwCU\Ck5HbLC73yEMQ3T CJMx.mp3.Syrk	Dropped File	61.38 KB	application/octet-stream	Access, Create, Write	CLEAN
db8fc48228dcf7032bf37633c20f3a1526333725f316e0e2b55ca3d19bf597e4	c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\eq95xs_2bmkwbb6.xls.syrk, C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\hfTktiwCU\Eq95Xs_2BMkWBb6.xls.Syrk	Dropped File	56.10 KB	application/octet-stream	Access, Create, Write	CLEAN
f35548e3840816ab1f22fccfc5d519b051b321e22cba0f2351d6e47ffa365ac2	c:\users\keecfmwgj\desktop\e06hth3voha0d\2 kc0zg1 rmrjok_gy.png.syrk, C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\2 KC0ZG1 RMrJoK_gY.png.Syrk	Dropped File	38.47 KB	application/octet-stream	Access, Create, Write	CLEAN
bfaa0a4a07452c90befba1c0f1e22cc3cc2974222f66321725aa614e6417df7e	c:\users\keecfmwgj\desktop\e06hth3voha0d\4o6jjgbzavbwsb6-29.png.syrk, C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\4o6jjgbzavbWSb6-29.png.Syrk	Dropped File	63.13 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dc838a4bdbc84dadab25864895e197ead4caf94974c41350561ac2a223e613a0	c:\users\keecfmwgj\desktop\e06hth3voha0d\5ifudwany.bmp.syrk, C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\5iFUDWANY.bmp.Syrk	Dropped File	49.57 KB	application/octet-stream	Access, Create, Write	CLEAN
03863fc164d35e106d1445e224f62223482049 61b1f6081117a390079330811e	C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BRmtCoyPLILg.jpg.Syrk, c:\users\keecfmwgj\desktop\e06hth3voha0d\brmtcoypllIg.jpg.syrk	Dropped File	1.80 KB	application/octet-stream	Access, Create, Write	CLEAN
9b1d46658d392bc49324587ab7f48ed7ebdab21aedf3e8edc1b84eb518258bb3	C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BtaCh0Rv1i6GNNdmI.png.Syrk, c:\users\keecfmwgj\desktop\e06hth3voha0d\btach0rv1i6gnndmi.png.syrk	Dropped File	18.25 KB	application/octet-stream	Access, Create, Write	CLEAN
88231ddcf7f2bf245d626949b0d93dfe4d65367eab25e5ad474b087723d9de28	C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\JhXCNVX54s7.png.Syrk, c:\users\keecfmwgj\desktop\e06hth3voha0d\jhxcnvx54s7.png.syrk	Dropped File	15.21 KB	application/octet-stream	Access, Create, Write	CLEAN
42abece8b8374ec41a384407d5a12b116dc74d1f27fa597a49114f09dd248acf	C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\OUWK.mp3.Syrk, c:\users\keecfmwgj\desktop\e06hth3voha0d\ouwk.mp3.syrk	Dropped File	4.38 KB	application/octet-stream	Access, Create, Write	CLEAN
ccd0b348a27958b4ea555a2ad7def37ba0c66ac96efde1022da0e6482c946bdb	c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\-8f.xls.syrk, C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\-8F.xls.Syrk	Dropped File	60.11 KB	application/octet-stream	Access, Create, Write	CLEAN
538ccda2d98e4b68f7b265316b72faf7237ceb535335f895447e9ebedaea4f24	C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\cDzt.ppt.Syrk, c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\cdzt.ppt.syrk	Dropped File	21.22 KB	application/octet-stream	Access, Create, Write	CLEAN
3214a38a14daecfea7d4f9030766aaa1aafc09e2f2dde2ae094f4ec09e908b6d	c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ncd4gg.jpg.syrk, C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\NcD4gg.jpg.Syrk	Dropped File	97.44 KB	application/octet-stream	Access, Create, Write	CLEAN
98ba79da92b6b14b87cb7a87ca80761780c5b4bde21143a7fe7ec552b262c8d9	c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\x7ay0560rvhbasv7.bmp.syrk, C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\X7aY0560rvhbASv7.bmp.Syrk	Dropped File	55.58 KB	application/octet-stream	Access, Create, Write	CLEAN
c859e8900eae6214d6c8a94f517d9cfb141e587024201aec72ebe8c006b0688e	c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ztjhwwr6z7cu6mtrpn.jpg.syrk, C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\ztjhWWR6z7cU6mtRPN.jpg.Syrk	Dropped File	21.43 KB	application/octet-stream	Access, Create, Write	CLEAN
ec188048930cc6cfd159cf00434a08653db076c0a3228c62e3814cd9c576a10b	C:\Users\kEecfMwgj\Desktop\4XirQCKnN-C5.mp3.Syrk, c:\users\keecfmwgj\desktop\4xirqcknn-c5.mp3.syrk	Dropped File	61.39 KB	application/octet-stream	Access, Create, Write	CLEAN
052c65ca957bcd04a26e04fe04d7dd538943060343aebcb3d21d8595baa22223	C:\Users\kEecfMwgj\Desktop\5wDjaVgryR0UBy6Yy26.gif.Syrk, c:\users\keecfmwgj\desktop\5wdjavgryr0uby6yy26.gif.syrk	Dropped File	50.55 KB	application/octet-stream	Access, Create, Write	CLEAN
bdddeb9d0c3b9b89cb2fbb3137a5f7fc617bf13cadca1d193f1a7502202cf078	c:\users\keecfmwgj\desktop\6t r wkg.pdf.syrk, C:\Users\kEecfMwgj\Desktop\6t r wKg.pdf.Syrk	Dropped File	44.71 KB	application/octet-stream	Access, Create, Write	CLEAN
95c750156132a986aa4168864e150db452ff15c579a83f959f72871795c12b6f	C:\Users\kEecfMwgj\Desktop\aYGQHCFalP7ms.bmp.Syrk, c:\users\keecfmwgj\desktop\aygqhcfalp7ms.bmp.syrk	Dropped File	35.61 KB	application/octet-stream	Access, Create, Write	CLEAN
6644778987660579834152e38b558fd54eb2c5931343139444713e9d955352fa	C:\Users\kEecfMwgj\Desktop\A_Xuo41AM2 4XZ.gif.Syrk, c:\users\keecfmwgj\desktop\a_xuo41am2 4xz.gif.syrk	Dropped File	66.57 KB	application/octet-stream	Access, Create, Write	CLEAN
6947b73d6cca5651f9134feb91dacf4b4080025f9cf3cc12e230d165ed28e3f6	C:\Users\kEecfMwgj\Desktop\bnnQ2Y.png.Syrk, c:\users\keecfmwgj\desktop\bnnq2y.png.syrk	Dropped File	15.38 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
61c6e143b3d888d07157b04c1fe42294e0c57c630cbd6eeaa7cb2026a0cb48f3	c:\users\keecfmwgj\desktop\ehz3w0f6qpam.png.syrk, C:\Users\kEecfMwgj\Desktop\EHZ3W0F6Qpam.png.Syrk	Dropped File	95.22 KB	application/octet-stream	Access, Create, Write	CLEAN
e574cd45c1530de4846b48ec68ccdf6d8f15a9d2458368575eebbd7bc79db7b7	C:\Users\kEecfMwgj\Desktop\KcV8WXd6gM.mp3.Syrk, c:\users\keecfmwgj\desktop\kcv8wxd6gm.mp3.syrk	Dropped File	83.24 KB	application/octet-stream	Access, Create, Write	CLEAN
78a0ed85c5f5dcd07142420b81df004eb51543322a6763dbc502f1e0980b7fea	c:\users\keecfmwgj\desktop\lfz_nda58jhfm.pdf.syrk, C:\Users\kEecfMwgj\Desktop\LfZ_NDA58Jhfm.pdf.Syrk	Dropped File	33.57 KB	application/octet-stream	Access, Create, Write	CLEAN
63a6b1e02d35d062e72ad252f605c7fba433d3cf7fb765155253461765bd06f2	c:\users\keecfmwgj\desktop\ltmu_vtfzdro.mp3.syrk, C:\Users\kEecfMwgj\Desktop\ltMu_vtFZDRo.mp3.Syrk	Dropped File	49.66 KB	application/octet-stream	Access, Create, Write	CLEAN
f1f1aa7a30c1fcd85a7cbf7d228f98876cbc44e280e5b75fcf7dad9bb559c2e5	c:\users\keecfmwgj\desktop\lw2zryjlbjcze.png.syrk, C:\Users\kEecfMwgj\Desktop\LW2ZryjLbjcZe.png.Syrk	Dropped File	54.30 KB	application/octet-stream	Access, Create, Write	CLEAN
c7ed925dd319a9c92df829ec65f1354d236d4de40e6b6f8ae52a61522fae8542	C:\Users\kEecfMwgj\Desktop\oSEF.xls.Syrk, c:\users\keecfmwgj\desktop\osef.xls.syrk	Dropped File	67.66 KB	application/octet-stream	Access, Create, Write	CLEAN
c40c4a1586e7838ad9a4c894c12173c08df382f53279931f20d3b4e09d0dc953	C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\2NDvK0UV6C93Or2y33.xls.Syrk, c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\2ndvk0uv6c93or2y33.xls.syrk	Dropped File	49.00 KB	application/octet-stream	Access, Create, Write	CLEAN
510ed9d07626dcee696852531b681fd35b0d812e2972c84b312085a9f6f39dcc	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\cptrf.ppt.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\CpTRf.ppt.Syrk	Dropped File	65.04 KB	application/octet-stream	Access, Create, Write	CLEAN
d84f4d69d5bb1879cf13bd80d0b1be638db6ccf91b1550f70e1c5e6b77f93cd8	C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\DgJ _YHDeXbtu1aaa9P7.pptx.Syrk, c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\dgj _yhdexbtu1aaa9p7.pptx.syrk	Dropped File	29.08 KB	application/octet-stream	Access, Create, Write	CLEAN
8a0de635eef6ae052bc93ea712423f362f8c6131f521656d929a85396c114488	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\ugbvvdin.pdf.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\uGb VVDiN.pdf.Syrk	Dropped File	42.72 KB	application/octet-stream	Access, Create, Write	CLEAN
677e6de07df80a6649d4974f22ac2dc9a0c0121e73420941275bcd91f2f306ac	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n_go2uxegr7yuru5exh\nfwtjiionnnx.ppt.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\n_Go2uXegR7yuru5EXh\nFwTJIloNnNX.ppt.Syrk	Dropped File	8.64 KB	application/octet-stream	Access, Create, Write	CLEAN
36450c6d7ff601cd6543fb38a6eecb0bb069063df3276d16038ba322d56c3f0e	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\appn7n4ht lo.pdf.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\apPn7N4hT Lo.pdf.Syrk	Dropped File	40.33 KB	application/octet-stream	Access, Create, Write	CLEAN
88b384a438a14086bfd3c7972cce6038c5f51a034973841fdc93f8a7a4894ce9	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\hd6yww0khas8.ppt.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\hd6YwW0KHas8.ppt.Syrk	Dropped File	51.27 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7aeca36cc1c2a8fb03e8bd8c5786f2ca7b1bd2e2702e5371a54a10cb29597249	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\mhccyt.docx.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\mHccYT.docx.Syrk	Dropped File	55.04 KB	application/octet-stream	Access, Create, Write	CLEAN
d69461131d88a15fbf64eba37702c8017c52f10066f2e7dc9fb431565c405101	c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n7u6-hdfzcmk12ax.ppt.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\n7u6-hdfZCMK12Ax.ppt.Syrk	Dropped File	5.25 KB	application/octet-stream	Access, Create, Write	CLEAN
c8d69816f228c5d92bcdef126b88f9f3f97ba0e92c999a96a4f7ef9c22667a94	C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9byo0\dP47.doc.Syrk, c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\tirkk9byo0\dp47.doc.syrk	Dropped File	17.38 KB	application/octet-stream	Access, Create, Write	CLEAN
b39e335595b51ec09e2a5c150bc968880c31079d2d2bc2afef1ac9a60a872644	C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9byo0\JGqHA5Ln0.ppt.Syrk, c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\tirkk9byo0\jgqha5ln0.ppt.syrk	Dropped File	97.18 KB	application/octet-stream	Access, Create, Write	CLEAN
e61b085fc26e324f42ae1360489eeb321c23cf2411d613123b429f8068bb963b	c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\j_xc70wda-y.xlsx.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\j_XC70WdA-Y.xlsx.Syrk	Dropped File	38.52 KB	application/octet-stream	Access, Create, Write	CLEAN
f482f765f278721fd2ca01a99d93bbeae83f8f879dd7971207fb0afef3e6cf23	C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\vztlNW.docx.Syrk, c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\vztlnw.docx.syrk	Dropped File	90.49 KB	application/octet-stream	Access, Create, Write	CLEAN
b44aae7dae20d884467694ee538427be6185cb745ecb213911fbf6fa9a4dc0ae	C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\n2mooDz97hNHy_Rw.doc.Syrk, c:\users\keecfmwgj\documents\gadgp30\qjecmq\z0wghk\n2moodz97hnhy_rw.doc.syrk	Dropped File	25.18 KB	application/octet-stream	Access, Create, Write	CLEAN
4d7694c5c927a5da321708a7bd50f069032af0e66d36f6e0293f551a6dfe2d02	C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\TiksC6kLaNE3N.ppt.Syrk, c:\users\keecfmwgj\documents\gadgp30\qjecmq\z0wghk\tiksc6klane3n.ppt.syrk	Dropped File	51.71 KB	application/octet-stream	Access, Create, Write	CLEAN
75275ef7e3aab964d0230a3818dcf3b17ee352a9b466b41b5d641a7fc856b141	c:\users\keecfmwgj\documents\gadgp30\qjecmq_e4_60ksbs_d7zx.pptx.syrk, C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ_E4_60KSBs_D7ZX.pptx.Syrk	Dropped File	14.14 KB	application/octet-stream	Access, Create, Write	CLEAN
ce69344077a84dcc4ba6f96737b7f1fa77c19b00c0f201ee76b3046ccd295ff5	c:\users\keecfmwgj\documents\0m2lwa6w2.docx.syrk, C:\Users\kEecfMwgj\Documents\0m2lWa6W2.docx.Syrk	Dropped File	87.30 KB	application/octet-stream	Access, Create, Write	CLEAN
abeb0eb440730f8fb3e4d815710bf52c0476b7b1709a6795e8c8f08aa293add5	C:\Users\kEecfMwgj\Documents\63C2JNBupUJaLCzjj.xlsx.Syrk, c:\users\keecfmwgj\documents\63c2jnbupujalczjj.xlsx.syrk	Dropped File	82.22 KB	application/octet-stream	Access, Create, Write	CLEAN
2928485fd3c9ef5962e3568e8237ec98bbac8740e91ee4508617c465166d0535	c:\users\keecfmwgj\documents\a_x_tiv5stl.docx.syrk, C:\Users\kEecfMwgj\Documents\A_x_tiv5stL.docx.Syrk	Dropped File	2.85 KB	application/octet-stream	Access, Create, Write	CLEAN
7c15b7aed4be5d19e36536841e39e0e3a8538ec0cce3842c05f32e3d7fb6c952	c:\users\keecfmwgj\documents\bx_hg08qccc73wa.pptx.syrk, C:\Users\kEecfMwgj\Documents\bx_hg08 qccc73wA.pptx.Syrk	Dropped File	64.44 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
30511e6572938110ef97c82fcfe6fc07d8d3e24b6ef1dd99af4b841e5f0921c7	C:\Users\kEecfMwgj\Documents\da4Yt5-_HXX-4.xlsx.Syrk, c:\users\keecfmwgj\documents\da4yt5-_hxx-4.xlsx.syrk	Dropped File	77.57 KB	application/octet-stream	Access, Create, Write	CLEAN
3ed68bb573ec4d31ab8dd78169813d36cc0c3e9c88dbf6c4fba0a137cecf0a97	C:\Users\kEecfMwgj\Documents\hiQyDV.pptx.Syrk, c:\users\keecfmwgj\documents\hiqydv.pptx.syrk	Dropped File	72.00 KB	application/octet-stream	Access, Create, Write	CLEAN
b94515d82ce9a82f4e67ce1f32cb50d12a579e9266dd9c84eeb042154696161c	C:\Users\kEecfMwgj\Documents\hQwa.pptx.Syrk, c:\users\keecfmwgj\documents\hqwa.pptx.syrk	Dropped File	91.99 KB	application/octet-stream	Access, Create, Write	CLEAN
b80401295bdac40e332fa7acd778d47b0ae3ca56f2840c236a06d2b4d960d8c9	C:\Users\kEecfMwgj\Documents\kLxyk2vrts2_ylshyl.xlsx.Syrk, c:\users\keecfmwgj\documents\klxyk2vrts2_ylshyl.xlsx.syrk	Dropped File	58.13 KB	application/octet-stream	Access, Create, Write	CLEAN
030ff19c62a6127b358e8a9462509a3bf6a4306dc1fb5c3a9dd44cfe87d2a2f4	c:\users\keecfmwgj\documents\kzkisarpnjyn.xlsx.syrk, C:\Users\kEecfMwgj\Documents\KZkiSaRpNjYn.xlsx.Syrk	Dropped File	44.58 KB	application/octet-stream	Access, Create, Write	CLEAN
8c16c1c0f353de3ec419054467c27dc78a96fa47464654e210bf24032373e553	C:\Users\kEecfMwgj\Documents\p9eQVmM.pptx.Syrk, c:\users\keecfmwgj\documents\p9eqvmm.pptx.syrk	Dropped File	61.68 KB	application/octet-stream	Access, Create, Write	CLEAN
24094bb37a0d069d23bda61d33474ba70e4378bd58d39994b64ffdbff858cada	c:\users\keecfmwgj\documents\qdt8j-_xcq 65llcpzig.pptx.syrk, C:\Users\kEecfMwgj\Documents\qDT8j-_Xcq 65lLCPzig.pptx.Syrk	Dropped File	29.71 KB	application/octet-stream	Access, Create, Write	CLEAN
276436b4dce497a38dca49137571beaa5824ef69f70cada037abfe9f77710a3e	C:\Users\kEecfMwgj\Documents\tbolTOBf6oytAdVf.xls.Syrk, c:\users\keecfmwgj\documents\tboltobf6oytadvf.xls.syrk	Dropped File	9.55 KB	application/octet-stream	Access, Create, Write	CLEAN
1279fd3acd75d1e5c6b29b4df9c001c72c581eb9cfba8d440267ceb269a79bd0	C:\Users\kEecfMwgj\Documents\tcbu3AshPzFcR2r8Ck o.docx.Syrk, c:\users\keecfmwgj\documents\tcbu3ashpzfcr2r8ck o.docx.syrk	Dropped File	57.30 KB	application/octet-stream	Access, Create, Write	CLEAN
42a99a78bf3011643889b6396a91de639f69a5ec963eb3ff76b7627a1397b6ca	C:\Users\kEecfMwgj\Documents\UYWqtSLk mI.docx.Syrk, c:\users\keecfmwgj\documents\uywqtslkmi.docx.syrk	Dropped File	80.25 KB	application/octet-stream	Access, Create, Write	CLEAN
c437d04f871e6424c828969fdeec8aa4509e5c6063f0c26478bf9d26c8f878a7	C:\Users\kEecfMwgj\Documents\yl14C.docx.Syrk, c:\users\keecfmwgj\documents\yl14c.docx.syrk	Dropped File	14.72 KB	application/octet-stream	Access, Create, Write	CLEAN
fdafe882325a70e738d50a846df931722fd4e1c59f19b6851b401e7c22471b6a	C:\Users\kEecfMwgj\Documents\zm9nla-NPD71l4thrEn.xls.Syrk, c:\users\keecfmwgj\documents\zm9nla-npd71l4thren.xls.syrk	Dropped File	32.33 KB	application/octet-stream	Access, Create, Write	CLEAN
2702f45ec0f378dd4ee634a4d4a700e87b71ac90ad56649cce14084d85e81215	C:\Users\kEecfMwgj\Documents\zVu_x.xlsx.Syrk, c:\users\keecfmwgj\documents\zvu_x.xlsx.syrk	Dropped File	49.85 KB	application/octet-stream	Access, Create, Write	CLEAN
6aed588650635d21c3e6b3ed5845e2c3c6c373efa37fcc5519c486a5b0080b98	C:\Users\kEecfMwgj\Music\M-QP9r3m\5q7ybWyiM4zx.wav.Syrk, c:\users\keecfmwgj\music\m-qp9r3m\5q7ybwyim4zx.wav.syrk	Dropped File	4.18 KB	application/octet-stream	Access, Create, Write	CLEAN
888f7edb6bf699754e29071bfc6167075ff6fc2d67ad8dedbdc974bc87696a23	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\0cA5darpWBXR.wav.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbufn\0ca5darpwbxr.wav.syrk	Dropped File	56.83 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
78b6fba081d323bf751f2406e692527359e3cc4506dc2595b88e01c0ee4acf5b	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbu fn\2-hxc4lfdhsq_mkvo.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\M5V7viLPSBu Fn\2-hXC4LFdHsq_mKvo.mp3.Syrk	Dropped File	19.10 KB	application/octet-stream	Access, Create, Write	CLEAN
525f3ccaa8a1da2f6fb0e2f000db446e903fd7c5c29c15d84420f867127eee15	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\M5V7viLPSBu Fn\UOrn1.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbu fn\uorn1.mp3.syrk	Dropped File	61.72 KB	application/octet-stream	Access, Create, Write	CLEAN
f2146e1641dc3a7f78f39b7002ced47a9ba62502a1c92951f5f71bbffbc574fc	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\M5V7viLPSBu Fn\XXq4gabRA0W.wav.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbu fn\xxq4gabra0w.wav.syrk	Dropped File	8.22 KB	application/octet-stream	Access, Create, Write	CLEAN
223f420922a8990ff59b429b0c90c35a811512649a3ce3972599e16e52bbd467	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\waroxvlp.wav.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\n8siGXFTdMtKcZh\wARoxvlp.wav.Syrk	Dropped File	37.11 KB	application/octet-stream	Access, Create, Write	CLEAN
9ab6a4c5ba3d6374398b51b1ca1f5904fde4cf58dafcb0dd23eb149f2c96df06	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\xu9kprwq9.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\n8siGXFTdMtKcZh\xU9kprwq9.mp3.Syrk	Dropped File	9.93 KB	application/octet-stream	Access, Create, Write	CLEAN
7f7296bab0b7169ea969fa7e8b0fcd6fcc43eb3151a6b854656054cd2b253733	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\n8siGXFTdMtKcZh\YBZFeG9.wav.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\ybzfeg9.wav.syrk	Dropped File	2.88 KB	application/octet-stream	Access, Create, Write	CLEAN
9e3742ea024c4b6a27ff7268b6f93acdd7686ab96f1da65d048bc05b3b72e84d	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\69v7zlnse_6kw0ym e.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\69V7ZlNsE_6KW0Ym e.mp3.Syrk	Dropped File	10.41 KB	application/octet-stream	Access, Create, Write	CLEAN
40319d1ce18c61ca89aee161b0690aa7321f60ed0499f36b3020fea8e3580f14	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\l9ni.wav.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\L9ni.wav.Syrk	Dropped File	67.18 KB	application/octet-stream	Access, Create, Write	CLEAN
1f7c93b5af11fa630b72a770b3f302dc531c9467ea6457b5cb41f5b3fbdebe06	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\sb2jvq1jz7zixzf4.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\SB2jVQ1jZ7ziXzf4.mp3.Syrk	Dropped File	82.18 KB	application/octet-stream	Access, Create, Write	CLEAN
bff18a4d12dc95648349c4c44c433a5883fb4685d31b393dae5ced79902db84d	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\O5Kq9mR4CC\ZDzv.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\zdzv.mp3.syrk	Dropped File	61.29 KB	application/octet-stream	Access, Create, Write	CLEAN
c6f41b3640d0ab7e302136137e890e33f53b1efe65554e0a3f207c5d008d0840	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdql3uzhk02\qL4ltMgKfKQ\-hsXLHPSE2Gpg.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\-hsxlhpse2gpg.mp3.syrk	Dropped File	72.07 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c01a20319d21070b2246e76ea0ea942882508c5f2603b40ff34eb1f6d2f52aa2	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\li_8a-uy.wav.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ItMgKfKQ\Li_8A-UY.wav.Syrk	Dropped File	40.50 KB	application/octet-stream	Access, Create, Write	CLEAN
450ed002f4b8c7f83e80c1e4976741808594d4d7cb523c304290af1e3bf19dbc	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ItMgKfKQ\RE3_9X-yu-SSwhMc.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\re3_9x-yu-sswhmc.mp3.syrk	Dropped File	32.86 KB	application/octet-stream	Access, Create, Write	CLEAN
0cea05e6120228dd58220ffb69a994b3d46b4aa2a40c64edd4400bc022557d05	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ItMgKfKQ\tjL0lG.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\tjl0lg.mp3.syrk	Dropped File	96.04 KB	application/octet-stream	Access, Create, Write	CLEAN
303c93e49ed05431382581da782e6299bae015e341293a7a0c1a322f3b9b84b8	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\u0af.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ItMgKfKQ\U0af.mp3.Syrk	Dropped File	76.52 KB	application/octet-stream	Access, Create, Write	CLEAN
06a9abde69f3d19c6a15070f9dfd43d364a378550c8c5c7538408d0651289292	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\xLkRw\MsuOsA4r023U.mp3.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\xlkrw\msuosa4r023u.mp3.syrk	Dropped File	52.49 KB	application/octet-stream	Access, Create, Write	CLEAN
3964603d995993e318e5f473494c0ed085ead3029f8d46f6ea7c921810ef0d6e	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\xlkrw\wwq2xl38e.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\xLkRw\Wwq2Xl38E.mp3.Syrk	Dropped File	91.39 KB	application/octet-stream	Access, Create, Write	CLEAN
2cbb2137ef5b8aa3f0540394e797ecc21b5928e74edfb7faa5b50025641f1dd8	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\i82ix5otq989c-uh2jwl.mp3.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\I82Ix5OTQ989c-Uh2jWL.mp3.Syrk	Dropped File	74.29 KB	application/octet-stream	Access, Create, Write	CLEAN
2ccb28df41fa02450046408495adc46b186989e5a02a6e356a1a332eb487e080	C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\jW54Ba8xSbY.wav.Syrk, c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\jw54ba8xsby.wav.syrk	Dropped File	10.30 KB	application/octet-stream	Access, Create, Write	CLEAN
09eca56ca95f5d48299d311ff5185519568f92ceadb9bff7086ce8436c7ceca2	c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ln8yfcu_yh0.wav.syrk, C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\ln8YfCU_Yh0.wav.Syrk	Dropped File	62.18 KB	application/octet-stream	Access, Create, Write	CLEAN
04d5e5f770e50d6961941f77bb31c5b9e7b2e8c33a17df9639c8553224b7881f	c:\users\keecfmwgj\music\m9te.wav.syrk, C:\Users\kEecfMwgj\Music\M9Te.wav.Syrk	Dropped File	24.47 KB	application/octet-stream	Access, Create, Write	CLEAN
40fef7c27c8142c89dc0a645de52f1a9be73228a4e187edb66191a161f98864b	C:\Users\kEecfMwgj\Music\MT00azHNzYeUklUK7WLY.wav.Syrk, c:\users\keecfmwgj\music\mt00azhnzyeukluk7wly.wav.syrk	Dropped File	92.82 KB	application/octet-stream	Access, Create, Write	CLEAN
596ed2ba26fc25b1ebe3108ae2ffd8fccd23024b2a0426b06008f8fd849d70a3	c:\users\keecfmwgj\music\omcoseo.wav.syrk, C:\Users\kEecfMwgj\Music\omCoSEo.wav.Syrk	Dropped File	99.55 KB	application/octet-stream	Access, Create, Write	CLEAN
055a52cf1872b7fa3dca042b79076567b8dd04821b79bc79696eb19b8ce505c5	c:\users\keecfmwgj\music\vazma_d1fuafei4nm_9.mp3.syrk, C:\Users\kEecfMwgj\Music\vAZMA_D1Fuafel4nm_9.mp3.Syrk	Dropped File	41.97 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
51d39d6cf54ba294edc2e1648bb85351a78c167748d96618e0d526b64cf07fde	c:\users\keecfmwgj\music\zern8svva2_nmg.mp3.syrk, C:\Users\kEecfMwgj\Music\ZERn8svVA2_nmG.mp3.Syrk	Dropped File	59.69 KB	application/octet-stream	Access, Create, Write	CLEAN
a5cdbcf0120cf4f97c13b0851956ff054b14f53b3517d5d19be090667df7fa6f	C:\Users\kEecfMwgj\Pictures\-20cBzLDzX_KXyz1k60.png.Syrk, c:\users\keecfmwgj\pictures\-20cbzldzx_kxyz1k60.png.syrk	Dropped File	40.49 KB	application/octet-stream	Access, Create, Write	CLEAN
03a92cee666c6930caceaaa407ce399e75d242c0d628fddfa16582870a0ee4fa	C:\Users\kEecfMwgj\Pictures\-lvNIlwLh6qJBQ7x.bmp.Syrk, c:\users\keecfmwgj\pictures\-lvnliwlh6qjbq7x.bmp.syrk	Dropped File	50.11 KB	application/octet-stream	Access, Create, Write	CLEAN
7659cb2d5739a47ee12cf6392c81822d5652712cb4d09761c2da4ede7770808f	c:\users\keecfmwgj\pictures\-yqu7r.jpg.syrk, C:\Users\kEecfMwgj\Pictures\-yqu7r.jpg.Syrk	Dropped File	96.85 KB	application/octet-stream	Access, Create, Write	CLEAN
eb0a5ab441858e6fc41007aa207d6501171706d969e24e1d321425a51991dc34	c:\users\keecfmwgj\pictures\09ijundbva.gif.syrk, C:\Users\kEecfMwgj\Pictures\09iJUNDbva.gif.Syrk	Dropped File	23.89 KB	application/octet-stream	Access, Create, Write	CLEAN
1f3f4ecf25f0e7b023b9cd44c358e10d198f2307deb96c0feeadbf9ba04c0a31	c:\users\keecfmwgj\pictures\1tp--jqrn7ickv.jpg.syrk, C:\Users\kEecfMwgj\Pictures\1Tp--JQrN7iCKV.jpg.Syrk	Dropped File	43.30 KB	application/octet-stream	Access, Create, Write	CLEAN
0088e1df8972886c8622e3d5f52f87f64e8c0db4c143a2c9161e44ea1cd25b0f	c:\users\keecfmwgj\pictures\2r7o-shzef3qr6zs_c.gif.syrk, C:\Users\kEecfMwgj\Pictures\2R7o-shzeF3qr6Zs_C.gif.Syrk	Dropped File	11.74 KB	application/octet-stream	Access, Create, Write	CLEAN
7f7a7fe5d43430c7825ffed2f3662fc2ef5b9cd60ebe46de6e7cf1251a44cfea	c:\users\keecfmwgj\pictures\3r8d3dnv_alj.jpg.syrk, C:\Users\kEecfMwgj\Pictures\3r8D3DNV_Alj.jpg.Syrk	Dropped File	46.27 KB	application/octet-stream	Access, Create, Write	CLEAN
172c950dbc41bf6ea2870227cbaad003646c259b27a022b63d67e42fcbf3f014	C:\Users\kEecfMwgj\Pictures\6ZfnhezHZzwofrnONF.jpg.Syrk, c:\users\keecfmwgj\pictures\6zfnhezhzzwofrnonf.jpg.syrk	Dropped File	67.14 KB	application/octet-stream	Access, Create, Write	CLEAN
a82ce3b9110193471f62f7e8aafb9799d7125a47ebe94bc71999986d32ace1eb	c:\users\keecfmwgj\pictures\8czrpcyd_m6g307p3uxk.png.syrk, C:\Users\kEecfMwgj\Pictures\8CzrpcYd_M6g307P3Uxk.png.Syrk	Dropped File	78.30 KB	application/octet-stream	Access, Create, Write	CLEAN
58a064d5257e3f2e145c09c0396e6c3413c9c1717659303b96ba85e879a690e6	C:\Users\kEecfMwgj\Pictures\8DVbrPzwsfunn.jpg.Syrk, c:\users\keecfmwgj\pictures\8dvbrpzwsfunn.jpg.syrk	Dropped File	51.33 KB	application/octet-stream	Access, Create, Write	CLEAN
3ed81e36b36c1dfded79352d4f5d84cd453c6b1fd9fffdcccc3c08edf50664d9	c:\users\keecfmwgj\pictures\bimh.png.syrk, C:\Users\kEecfMwgj\Pictures\BiMH.png.Syrk	Dropped File	41.89 KB	application/octet-stream	Access, Create, Write	CLEAN
4344ca461620c066747fe78180686ffa952030ee43584cc4a9d897c5374191f4	C:\Users\kEecfMwgj\Pictures\CRAGPLrxjBWjbAs_pS.jpg.Syrk, c:\users\keecfmwgj\pictures\cragplrxjbwjbas_ps.jpg.syrk	Dropped File	6.25 KB	application/octet-stream	Access, Create, Write	CLEAN
9315c9391bf0c43e01475bccee8a530041d3d2626b7f8013abe32e4d58c68cce	C:\Users\kEecfMwgj\Pictures\dLcXhG3aWfBaiR.gif.Syrk, c:\users\keecfmwgj\pictures\dlcxhg3awfbair.gif.syrk	Dropped File	24.79 KB	application/octet-stream	Access, Create, Write	CLEAN
2489cd2c6a01050aaac1f6cba713f712d6f6efd5583304c09c76e6383a430bbf	C:\Users\kEecfMwgj\Pictures\F-RYQ.jpg.Syrk, c:\users\keecfmwgj\pictures\f-ryq.jpg.syrk	Dropped File	34.27 KB	application/octet-stream	Access, Create, Write	CLEAN
5516ef7b3486c11ef001d9013dc0f278a48975d59c85fb75f0688f897d84be6c	C:\Users\kEecfMwgj\Pictures\gJaInSM9o_s.jpg.Syrk, c:\users\keecfmwgj\pictures\gjaInsm9o_s.jpg.syrk	Dropped File	13.96 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e297a17c99bbed4c0963db8287a5ff390247d03a72a060ad0c04a2c523f5eab8	c:\users\keecfmwgj\pictures\gm5d9kgelxbt.png.syrk, C:\Users\kEecfMwgj\Pictures\gM5d9KgElxbt.png.Syrk	Dropped File	26.68 KB	application/octet-stream	Access, Create, Write	CLEAN
354508e4b82a4b0d81e45955855efd853ef2426a5035a7e715218e537a97ecfb	c:\users\keecfmwgj\pictures\gn4io1vv8uthsx.png.syrk, C:\Users\kEecfMwgj\Pictures\Gn4IO1VV8utHsX.png.Syrk	Dropped File	31.29 KB	application/octet-stream	Access, Create, Write	CLEAN
a201b847758164f63c76bcae9584f04c01387aee3820073e66782596ae6dbc2a	C:\Users\kEecfMwgj\Pictures\hwQvkSY6qlajdf.jpg.Syrk, c:\users\keecfmwgj\pictures\hwqvksy6qiajdf.jpg.syrk	Dropped File	41.50 KB	application/octet-stream	Access, Create, Write	CLEAN
9f048704fbaac9839cc4b459954c1eca325431f89738c5e65332d7090485a8ab	c:\users\keecfmwgj\pictures\ie3k6n7c0_b gizgjbf-.png.syrk, C:\Users\kEecfMwgj\Pictures\IE3K6N7c0_b GIZGjbF-.png.Syrk	Dropped File	45.43 KB	application/octet-stream	Access, Create, Write	CLEAN
0fb0a7c611b7597d1b1f57b1d9433e05cc08f835100ca48babba4913dd43de1b	C:\Users\kEecfMwgj\Pictures\JhqgivuCmr9tbit.jpg.Syrk, c:\users\keecfmwgj\pictures\jhqgivucmr9tbit.jpg.syrk	Dropped File	59.04 KB	application/octet-stream	Access, Create, Write	CLEAN
77553e052f0a975911da42aedc8e0bf2196f346c820208d6391ec7d82a89b507	C:\Users\kEecfMwgj\Pictures\kwI_sPi1.png.Syrk, c:\users\keecfmwgj\pictures\kwi_spi1.png.syrk	Dropped File	36.94 KB	application/octet-stream	Access, Create, Write	CLEAN
d5f92769e115d0d64574d5cee2e7d44b96d01bde5ac2525de988c09de5541283	C:\Users\kEecfMwgj\Pictures\LxEyCMb3cz G.png.Syrk, c:\users\keecfmwgj\pictures\lxeycmb3czg.png.syrk	Dropped File	94.74 KB	application/octet-stream	Access, Create, Write	CLEAN
5baaa1665fc5fcf36c9bce0a070a4083cc594e1a83cd5e3109e4a7c7dd9ba9ea	C:\Users\kEecfMwgj\Pictures\mh_2oAjD6lQO.gif.Syrk, c:\users\keecfmwgj\pictures\mh_2oajd6iqo.gif.syrk	Dropped File	39.64 KB	application/octet-stream	Access, Create, Write	CLEAN
05f38573d14f446971064b7c2532d797739fefbfe7489b6fbf4225f019df8abc	c:\users\keecfmwgj\pictures\neejrl4diryjsv.bmp.syrk, C:\Users\kEecfMwgj\Pictures\NEEjRL4DiRYJSV.bmp.Syrk	Dropped File	12.27 KB	application/octet-stream	Access, Create, Write	CLEAN
4190bc07768212b18635d98fe68ce1c1d5bf1e1ca19003b72039c460b757149f	c:\users\keecfmwgj\pictures\qjmibj2csojvn7un2o.bmp.syrk, C:\Users\kEecfMwgj\Pictures\QJMIbj2cSoJVN7un2O.bmp.Syrk	Dropped File	37.07 KB	application/octet-stream	Access, Create, Write	CLEAN
c865cb57a3d943ed2135b8e0e790bfbaf0a67d75ec0eb38f0d92374094a5b3a2	C:\Users\kEecfMwgj\Pictures\qNxgBCMJFfZZ 6.bmp.Syrk, c:\users\keecfmwgj\pictures\qnxgbcmjffzz 6.bmp.syrk	Dropped File	17.63 KB	application/octet-stream	Access, Create, Write	CLEAN
1c5b84a5d5ce04fd6a066ee035ed2fe73ce4ccaf16e1ad55aa298256adb78c05	C:\Users\kEecfMwgj\Pictures\rokbMHY7.bmp.Syrk, c:\users\keecfmwgj\pictures\rokbmhy7.bmp.syrk	Dropped File	43.80 KB	application/octet-stream	Access, Create, Write	CLEAN
6a004621590e48d14fc76093da6e81edeb39ae27342b8504284f9ebe091fc098	C:\Users\kEecfMwgj\Pictures\tBNEwownJMNLIH-.gif.Syrk, c:\users\keecfmwgj\pictures\tbnewownjmnlih-.gif.syrk	Dropped File	44.72 KB	application/octet-stream	Access, Create, Write	CLEAN
49d147b5cdc9df105c880b372f8dbc18458d7585026d3e749528132e1ccd524c	c:\users\keecfmwgj\pictures\tfnlk0smrt1_1xww.gif.syrk, C:\Users\kEecfMwgj\Pictures\TfnLK0sMrt1_1XwW.gif.Syrk	Dropped File	29.36 KB	application/octet-stream	Access, Create, Write	CLEAN
654070e295114ae7dcd103d1898fb060b0d719e099b0110f0981eb4f479194e4	c:\users\keecfmwgj\pictures\t_v5c6i.png.syrk, C:\Users\kEecfMwgj\Pictures\t_v5C6i.png.Syrk	Dropped File	81.54 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
49e1a97172dd5b92de31bee589c86752e112dfb3a3287fb4dde06c67e839b347	C:\Users\kEecfMwgj\Pictures\ut5l85Hmrtdjra4F.jpg.Syrk, c:\users\keecfmwgj\pictures\ut5i85hmrtdjra4f.jpg.syrk	Dropped File	8.27 KB	application/octet-stream	Access, Create, Write	CLEAN
2ddac7b33946bf2158d4b6c543f5aaf860d4b32bac502fd58e6101c2ec6dc7b7	c:\users\keecfmwgj\pictures\uz-c.gif.syrk, C:\Users\kEecfMwgj\Pictures\uZ-c.gif.Syrk	Dropped File	62.24 KB	application/octet-stream	Access, Create, Write	CLEAN
2092b2bf529afcefc0eae35505ece1403ac3c783d59700d4d1399d512d671f1a	C:\Users\kEecfMwgj\Pictures\v30MfWJ0Z.jpg.Syrk, c:\users\keecfmwgj\pictures\v30mfwj0z.jpg.syrk	Dropped File	28.16 KB	application/octet-stream	Access, Create, Write	CLEAN
2dd901e5cc1444d7d97dadef2ab6ab852ec942b45009c6c82a0183510c69a912	C:\Users\kEecfMwgj\Pictures\XOXL0s.gif.Syrk, c:\users\keecfmwgj\pictures\xoxl0s.gif.syrk	Dropped File	75.82 KB	application/octet-stream	Access, Create, Write	CLEAN
9a890251708b8caabb2ec2e4f53df7cc4772321016181f2f1ea658f74231551d	c:\users\keecfmwgj\pictures\ya649h.jpg.syrk, C:\Users\kEecfMwgj\Pictures\yA649h.jpg.Syrk	Dropped File	24.71 KB	application/octet-stream	Access, Create, Write	CLEAN
24e509d3f3df4cb17ad3350892c541c59de7465df67406d4eef4ed3a5e46f2cb	c:\users\keecfmwgj\videos\gjgfz-.mp4.syrk, C:\Users\kEecfMwgj\Videos\gJgFz-.mp4.Syrk	Dropped File	66.36 KB	application/octet-stream	Access, Create, Write	CLEAN
85e271c0eda333f5c00242ec7482cd2125cf59e31ac6966ac57f83a8260fbf31	c:\users\keecfmwgj\videos\h1j7hblziw7l.avi.syrk, C:\Users\kEecfMwgj\Videos\H1J7hBLzIW7L.avi.Syrk	Dropped File	19.32 KB	application/octet-stream	Access, Create, Write	CLEAN
836eb1d2d7b9d1e283807b30246dca0ee2298dfe42274df44b50eacd1d9ef812	C:\Users\kEecfMwgj\Videos\qgeTWMdHrM.mp4.Syrk, c:\users\keecfmwgj\videos\qgetwmdhrm.mp4.syrk	Dropped File	81.52 KB	application/octet-stream	Access, Create, Write	CLEAN
ccf26473d57d5e41910278dba046e038ac7fa80fa2975514d2b8db837ab9c20b	c:\users\keecfmwgj\videos\qpxgrgh9_6h.avi.syrk, C:\Users\kEecfMwgj\Videos\Qpxgrgh9_6H.avi.Syrk	Dropped File	64.29 KB	application/octet-stream	Access, Create, Write	CLEAN
5c5d16bed3ebf999377f7a62c8e3750efd043369cff963604e2ef4321a24c55c	C:\Users\kEecfMwgj\Videos\TXd5XhbVM_gRmGa.mp4.Syrk, c:\users\keecfmwgj\videos\txd5xhbvm_grmga.mp4.syrk	Dropped File	25.13 KB	application/octet-stream	Access, Create, Write	CLEAN
365f0ae6285dc9f0d469e51f458e33ce2702ed53fe4b6f3230f06275045b08ba	c:\users\keecfmwgj\videos\ulsd6hewxcm_chkzb.avi.syrk, C:\Users\kEecfMwgj\Videos\uLsd6HEWXCm_CHkZB.avi.Syrk	Dropped File	44.44 KB	application/octet-stream	Access, Create, Write	CLEAN
10663e99ff5e295979fe779f776bbc53b07896be38d142ba39d5b64fb3636047	c:\users\keecfmwgj\videos\wctn_hgh2xhblipzt0o.avi.syrk, C:\Users\kEecfMwgj\Videos\wCtn_HGh2XHBliPZt0O.avi.Syrk	Dropped File	7.18 KB	application/octet-stream	Access, Create, Write	CLEAN
8652ba9110046eeebf36fec821690dbca5ab0cf701781fecff50adb651e13f74	c:\users\keecfmwgj\videos\xbhxbnsb3poh.mp4.syrk, C:\Users\kEecfMwgj\Videos\xbhXbnSb3PoH.mp4.Syrk	Dropped File	91.02 KB	application/octet-stream	Access, Create, Write	CLEAN
7e5c0a4b50179f0ae93ad46813441b2e55fdb59b6bd5eddbd450c21aa485ee28	c:\users\keecfmwgj\videos\xleaz.mp4.syrk, C:\Users\kEecfMwgj\Videos\XLEaz.mp4.Syrk	Dropped File	49.14 KB	application/octet-stream	Access, Create, Write	CLEAN
89d1489cc425cd1fde3a36222517150aa70d5278d9d20f0d95a5600c19aeb06e	C:\Users\kEecfMwgj\Videos\YZQR06gE.avi.Syrk, c:\users\keecfmwgj\videos\yzqr06ge.avi.syrk	Dropped File	79.35 KB	application/octet-stream	Access, Create, Write	CLEAN
039c8f3ed3deef27c1dfbdd3a54221a0650df6532290177eb3edc81b4e512f40	c:\users\keecfmwgj\videos\z8vxfzj-jnzgo.mp4.syrk, C:\Users\kEecfMwgj\Videos\Z8vxFZJ-jnzGO.mp4.Syrk	Dropped File	19.33 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
57fcc7081a456cfee4e3e0752d88f3d18e2fd82b76186f70e76829ca2b3dbf6b	c:\users\keecfmwgj\videos\zhli4r.mp4.syrk, C:\Users\kEecfMwgj\Videos\ZHli4r.mp4.Syrk	Dropped File	1.61 KB	application/octet-stream	Access, Create, Write	CLEAN
dca72b1d0a3327a56de391757ba37e384359876ac3d1e3d3c10f2e8f8b4b2d1d	C:\Users\kEecfMwgj\Desktop\Readme_now.txt	Dropped File	234 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\Setup.exe	Accessed File, Sample File	Access	MALICIOUS
c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\ck5hblc73yemq3tcjmx.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\e06hth3voha0d\hftktiwcu\eq95xs_2bmkwbb6.xls.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\e06hth3voha0d\2 kc0zg1 rmrjok_gy.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\e06hth3voha0d\4o6jjgbzavbwsb6-29.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\e06hth3voha0d\5ifudwany.bmp.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BRmtCoyPLlLg.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\BtaCh0Rv1i6GNNdmI.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\JhXCNVX54s7.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\E06hTH3VoHA0d\OUWK.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\-8f.xls.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\M3w-Q0RZrFUkL\cDzt.ppt.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ncd4gg.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\x7ay0560rvhbasv7.bmp.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\m3w-q0rzrfukl\ztjhwwr6z7cu6mtrpn.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\4XirQCKnN-C5.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\5wD jaVgryR0UBy6Yy26.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\6t r wkg.pdf.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\aYGQHCFalP7ms.bmp.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\A_Xuo41AM2 4XZ.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\bnnQ2Y.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ehz3w0f6qpam.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\KcV8WXd6gM.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\lf z_nda58jhfm.pdf.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ltmu_vt fzdro.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\lw2zryjl bjcze.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\oSEF.xls.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\2NDvK0UV6C93Or2y33.xls.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\cptrf.ppt.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\ahvIkv6BhGP\9dBEoJADWjyNbxb\DgJ _YHDeXbtu1aaa9P7.pptx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\9dbeojadwjynbxb\ugb vvdin.pdf.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n_go2 uxegr7yuru5exh\nfwtjiionnnx.ppt.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\appn7n4ht lo.pdf.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\hd6yww0khas8.ppt.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\mhccyt.docx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\ahvikv6bhgp\n7u6-hdfzcmk12ax.ppt.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9 byo0\dP47.doc.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\tirKK9 byo0\JGqHA5Ln0.ppt.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\qjecmq\9bdyanhq-v\j_xc70wda-y.xlsx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\9bDYANhq-V\vztlNW.docx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\n2mooDz97hN Hy_Rw.doc.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\gADgp30\qJEcmQ\Z0wgHK\TiksC6kLaNE3N.ppt.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gadgp30\qjecmq_e4_60ksbs_d7zx.pptx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\0m2lwa6w2.docx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\63C2JNBupUJaLCzjj.xlsx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\a_x_tiv5stl.docx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\bx_hg08 qccc73wa.pptx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\da4Yt5-_HXX-4.xlsx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hiQyDV.pptx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hQwa.pptx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\kLxyk2vrts2_ylshyl.xlsx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\kzkisarpnjyn.xlsx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\p9eQVmM.pptx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\qdt8j-_xcq 65llcpzig.pptx.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents\tbolTOBf6oytAdVf.xls.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\tcbu3AshPzFcR2r8Ck o.docx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\UYWqtSLk mI.docx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\yl14C.docx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\zm9nla-NPD71l4thrEn.xls.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\zVu_x.xlsx.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\M-QP9r3m\5q7ybWyiM4zx.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\0cA5darpWBXR.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\m5v7vilpsbufn\2-hxc4lfdhsq_mkvo.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\UOrn1.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\M5V7viLPSBuFn\XXq4gabRA0W.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\waroxvlp.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\n8sigxftdmtkczh\xu9kprwq9.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\O5Kq9mR4CC\n8siGXFTdMtKcZh\YBZFeG9.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\69v7zInse_6kw0ym e.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\l9ni.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\o5kq9mr4cc\sb2jvq1jz7zixzf4.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\O5Kq9mR4CC\ZDzv.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\-hsXLHPSE2Gpg.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\li_8a-uy.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\RE3_9X-yu-SSwhMc.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\qL4ltMgKfKQ\tjL0lG.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ql4itmgkfkq\u0af.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\xLkRw\MsuOsA4r0 23U.mp3.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\xlkrw\wwq2xl38e.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\i82ix5otq989c-uh2jwl.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sR45lfBmn\HnGdqI3uzhk02\jW54Ba8xSbY.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\sr45lfbmn\hngdqi3uzhk02\ln8yfcu_yh0.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\m9te.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\MT00azHNzYeUklUK7WLY.wav.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\omcoseo.wav.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\vazma_d1fuafei4nm_9.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\zern8svva2_nmg.mp3.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\-20cBzLDzX_KXyz1k60.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\-IvNIIwLh6qJBQ7x.bmp.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\-yqu7r.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\09ijundbva.gif.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\1tp--jqrn7ickv.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\2r7o-shzef3qr6zs_c.gif.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\3r8d3dnv_alj.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\6ZfnhezHZzwofrnONF.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\8czrpcyd_m6g307p3uxk.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\8DVbrPzwsfunn.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\bimh.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CRAGPLrxjBWjbAs_pS.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\dLcXhG3aWfBaiR.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\F-RYQ.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\gJalnSM9o_s.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\gm5d9kgelxbt.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\gn4io1vv8uthsx.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\hwQvkSY6qlajdf.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ie3k6n7c0_b gizgjbf-.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\JhqgivuCmr9tbit.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\kwI_sPi1.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\LxEyCMb3cz G.png.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\mh_2oAjD6lQO.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\neejrl4diryjsv.bmp.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\qjmibj2csojvn7un2o.bmp.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\qNxgBCMJFfZZ 6.bmp.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Pictures\rokbMHY7.bmp.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\tBNEwownJMNLIH-.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\tfnlk 0smrt1_1xww.gif.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\t_ v5c6i.png.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ut5l85Hmrtdjra4F.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\uz- c.gif.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\v30MfWJ0Z.jpg.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\XOXL0s.gif.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\y a649h.jpg.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\gjgfz-.mp4.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\h1j7hblziw7l.avi.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\qgeTWMdHrM.mp4.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\qpxgrgh9_6h.avi.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\TXd5XhbVM_gRmGa.mp4.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\ulsd6hewxcm_chkzb.avi.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\wctn_hgh2xhblipzt0o.avi.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\xbhxbnsb3poh.mp4.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\xleaz.mp4.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\YZQR06gE.avi.Syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z8vxfzj-jnzgo.mp4.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\zhli4r.mp4.syrk	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	-	CLEAN
C:\Users\Public\Documents\cgo46ea565sdfse7.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\Public\Documents\startSF.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB5.tmp	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.bat	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
Cipher.psm1	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\Public\Documents\LimeUSB_Csharp.exe	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\Microsoft\+dp-.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\Default\AppData\Local\Microsoft\-pw+.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\Default\AppData\Local\Microsoft\-i+.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\kEecfMwgj\Desktop\Readme_now.txt	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
gr9wgs94fg5sb3y8l[.]000webhostapp[.]com	145.14.144.29	Germany	DNS	CLEAN
us-east-1[.]route-1[.]000webhost[.]awex[.]io	145.14.144.29	Germany	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
::f	-	-	-	CLEAN
::c	-	-	-	CLEAN
::	-	-	-	CLEAN
145.14.144.29	gr9wgs94fg5sb3y8l[.]000webhostapp[.]com, us-east-1[.]route-1[.]000webhost[.]awex[.]io	Germany	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	write, read, access	setup.exe	MALICIOUS
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	write, read, access	limeusb_csharp.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	setup.exe, powershell.exe, limeusb_csharp.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	setup.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender	access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	write, read, access	setup.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	setup.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop	access	setup.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop\WallpaperStyle	write, read, access	setup.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop\TileWallpaper	write, read, access	setup.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	access	limeusb_csharp.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt	write, read, access	limeusb_csharp.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	read, access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\ProtectedEventLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	read, access	powershell.exe	CLEAN

Process

Process Name	Commandline	Verdict
setup.exe	"C:\Users\kEecfMwgj\Desktop\Setup.exe"	MALICIOUS
startsf.exe	"C:\Users\Public\Documents\startSF.exe"	MALICIOUS
powershell.exe	powershell -ExecutionPolicy ByPass -File C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1	SUSPICIOUS
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	SUSPICIOUS
cgo46ea565sdfse7.exe	"C:\Users\Public\Documents\cgo46ea565sdfse7.exe"	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c cmd.exe /c mkdir %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher & cd %USERPROFILE%\Docume... ...nmail.com to recover them.' ^> $home\Desktop\Readme_now.txt >> cry.ps1 & echo start $home\Desktop\Readme_now.txt >> cry.ps1 & exit	CLEAN
cmd.exe	"C:\Windows\sysnative\cmd" /c "C:\Users\kEecfMwgj\AppData\Local\Temp\EDB2.tmp\EDB3.tmp\EDB4.bat C:\Users\Public\Documents\startSF.exe"	CLEAN
cmd.exe	cmd.exe /c mkdir C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c cmd.exe /c cd %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher & echo Remove-Item -path $ho... ...\Cipher\cry.ps1 & powershell -ExecutionPolicy ByPass -File %USERPROFILE%\Documents\WindowsPowerShell\Modules\Cipher\cry.ps1 & exit	CLEAN
cmd.exe	cmd.exe /c cd C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules\Cipher	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN

Process Name	Commandline	Verdict
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\kEecfMwgj\Desktop\Readme_now.txt	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN
limeusb_csharp.exe	"C:\Users\Public\Documents\LimeUSB_Csharp.exe"	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	windows 7 (64bit SP1 -EN- MSO_2016)
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	2023.4.1
Dynamic Engine Version	2023.4.1 / 11/10/2023 05:23
Static Engine Version	2023.4.1.0 / 2023-11-10 04:00:12
AV Exceptions Version	2023.4.1.4 / 2023-09-25 17:49:30
Link Detonation Heuristics Version	2023.4.1.48 / 2023-11-30 16:07:35
Smart Memory Dumping Rules Version	2023.4.1.4 / 2023-09-25 17:49:30
Config Extractors Version	2023.4.1.48 / 2023-11-30 16:07:35
Signature Trust Store Version	2023.4.1.4 / 2023-09-25 17:49:30
VMRay Threat Identifiers Version	2023.4.1.56 / 2023-12-06 21:36:31
YARA Built-in Ruleset Version	2023.4.1.48

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