MALICIOUS

Classifications: Wiper

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**adobloc.exe**
ID	#10437895
MD5	261a56d36006f274a3def7e2b0acb9d4
SHA1	3c6658e71b4b3a9c2200cf4c5cb337e1ebf449f4
SHA256	3e52c075a8eca95630727281a1380b78ac5392a035aef34aa3761afd1348e9f1
File Size	4218.89 KB
Report Created	2024-05-15 20:21 (UTC+2)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 67 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #30) rdhj0cnfevzx% deletes multiple user files.			
4/5	Masquerade	Uses a double file extension	1	-
	• File "C:\Users\RDhJ0CNFevzX\Desktop\oZDIZ.docx.exe" has a double file extension.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• The sample itself is a known malicious file.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #10) cmd.exe tries to detect 360TotalSecurity by file artifact.			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #14) ipconfig.exe reads the network adapters' addresses by API. • (Process #37) ipconfig.exe reads the network adapters' addresses by API.			
2/5	Discovery	Searches for sensitive browser data	1	-
	• (Process #10) cmd.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Discovery	Searches for sensitive FTP data	1	-
	• (Process #10) cmd.exe searches for sensitive data of FTP application "Total Commander" by file.			
2/5	Discovery	Searches for sensitive application data	1	-
	• (Process #10) cmd.exe searches for sensitive data of application "Windows Unattended Install" by file.			
1/5	Defense Evasion	Accesses volumes directly	7	-
	• (Process #1) adobloc.exe opens a handle to directly access the volume "C". • (Process #2) devoptisys.exe opens a handle to directly access the volume "C". • (Process #3) rdhj0cnfevzx% opens a handle to directly access the volume "C". • (Process #6) rdhj0cnfevzx% opens a handle to directly access the volume "C". • (Process #10) cmd.exe opens a handle to directly access the volume "C". • (Process #30) rdhj0cnfevzx% opens a handle to directly access the volume "C". • (Process #53) rdhj0cnfevzx% opens a handle to directly access the volume "C".			
1/5	Persistence	Installs system startup script or application	3	-
	• (Process #1) adobloc.exe adds "C:\IntelprocSB\devoptisys.exe" to Windows startup via registry. • (Process #1) adobloc.exe adds "C:\KaVBJI\dobaec.exe" to Windows startup via registry. • (Process #4) devoptisys.exe adds "C:\KaVBJI\dobaec.exe" to Windows startup via registry.			
1/5	Discovery	Enumerates running processes	9	-

Score	Category	Operation	Count	Classification
		• (Process #1) adobloc.exe enumerates running processes. • (Process #2) devoptisys.exe enumerates running processes. • (Process #3) rdhj0cnfevzx% enumerates running processes. • (Process #4) devoptisys.exe enumerates running processes. • (Process #5) dobaec.exe enumerates running processes. • (Process #6) rdhj0cnfevzx% enumerates running processes. • (Process #8) devoptisys.exe enumerates running processes. • (Process #30) rdhj0cnfevzx% enumerates running processes. • (Process #53) rdhj0cnfevzx% enumerates running processes.		
1/5	Hide Tracks	Creates process with hidden window	25	-
		• (Process #1) adobloc.exe starts (process #2) devoptisys.exe with a hidden window. • (Process #3) rdhj0cnfevzx% starts Anonymous Process with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #8) devoptisys.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #9) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #10) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #16) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #18) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #20) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #22) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #24) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #26) cmd.exe with a hidden window. • (Process #6) rdhj0cnfevzx% starts (process #28) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #31) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #32) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #34) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #39) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #41) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #42) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #43) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #44) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #45) cmd.exe with a hidden window. • (Process #30) rdhj0cnfevzx% starts (process #46) cmd.exe with a hidden window. • (Process #53) rdhj0cnfevzx% starts (process #54) cmd.exe with a hidden window. • (Process #53) rdhj0cnfevzx% starts (process #55) cmd.exe with a hidden window. • (Process #53) rdhj0cnfevzx% starts (process #56) cmd.exe with a hidden window.		
1/5	Obfuscation	Resolves API functions dynamically	9	-
		• (Process #1) adobloc.exe resolves 97 API functions by name. • (Process #2) devoptisys.exe resolves 97 API functions by name. • (Process #3) rdhj0cnfevzx% resolves 97 API functions by name. • (Process #4) devoptisys.exe resolves 97 API functions by name. • (Process #5) dobaec.exe resolves 97 API functions by name. • (Process #6) rdhj0cnfevzx% resolves 97 API functions by name. • (Process #8) devoptisys.exe resolves 97 API functions by name. • (Process #30) rdhj0cnfevzx% resolves 97 API functions by name. • (Process #53) rdhj0cnfevzx% resolves 97 API functions by name.		
1/5	Execution	Drops PE file	2	-

Score	Category	Operation	Count	Classification
		• (Process #1) adobloc.exe drops file "C:\IntelprocSB\devoptisys.exe". • (Process #1) adobloc.exe drops file "C:\KaVBJI\dobaec.exe".		
1/5	Execution	Executes dropped PE file	3	-
		• Executes dropped file "C:\Users\RDhJ0CNFevzX%". • Executes dropped file "C:\IntelprocSB\devoptisys.exe". • Executes dropped file "C:\KaVBJI\dobaec.exe".		
-	Trusted	Known clean file	1	-
		• Embedded file "" is a known clean file.		

Mitre ATT&CK Matrix

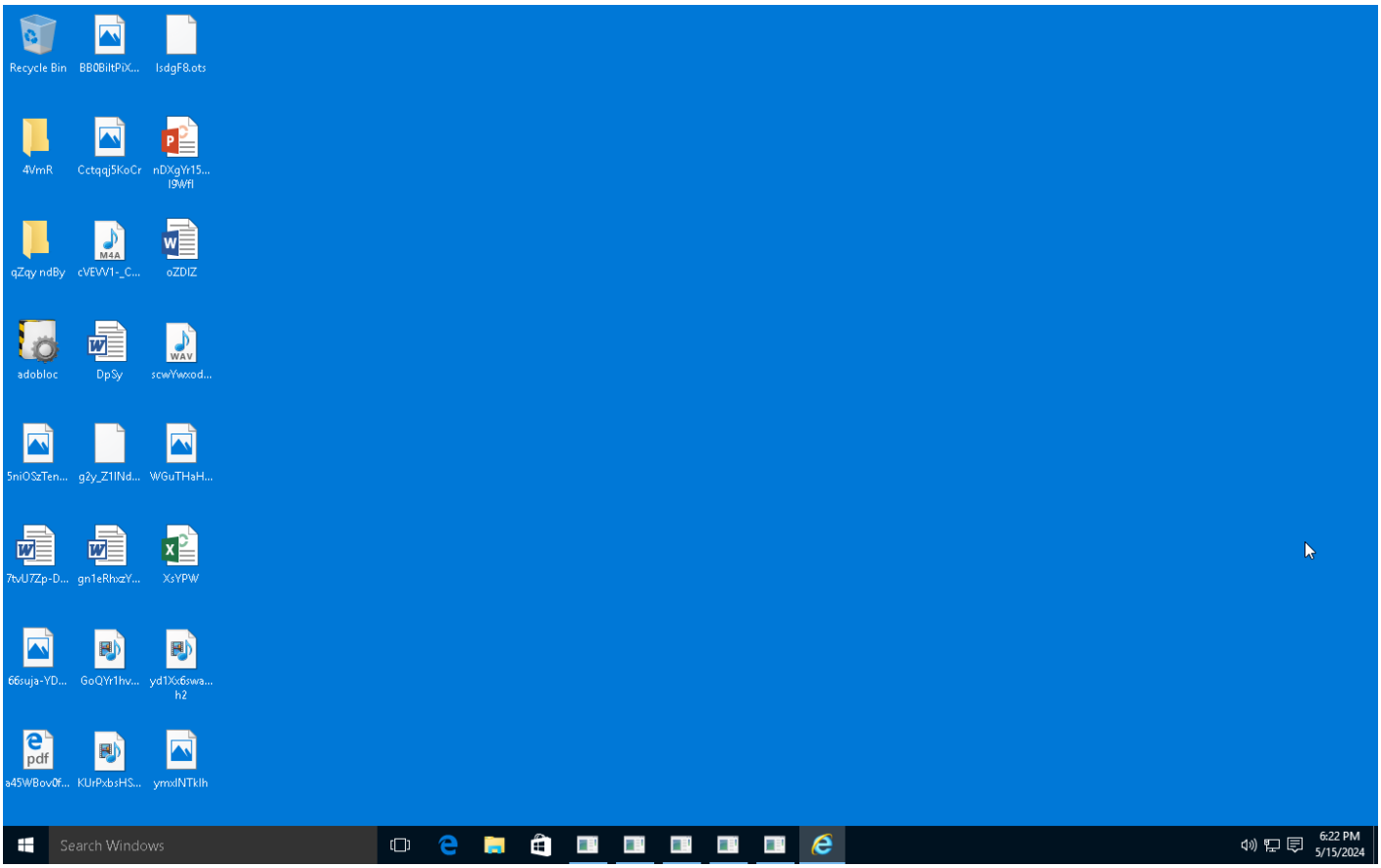
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1006 File System Logical Offsets	#T1081 Credentials in Files	#T1057 Process Discovery		#T1119 Automated Collection			#T1485 Data Destruction
				#T1112 Modify Registry		#T1016 System Network Configuration Discovery		#T1005 Data from Local System			
				#T1143 Hidden Window		#T1063 Security Software Discovery					
				#T1036 Masquerading		#T1083 File and Directory Discovery					
				#T1045 Software Packing							

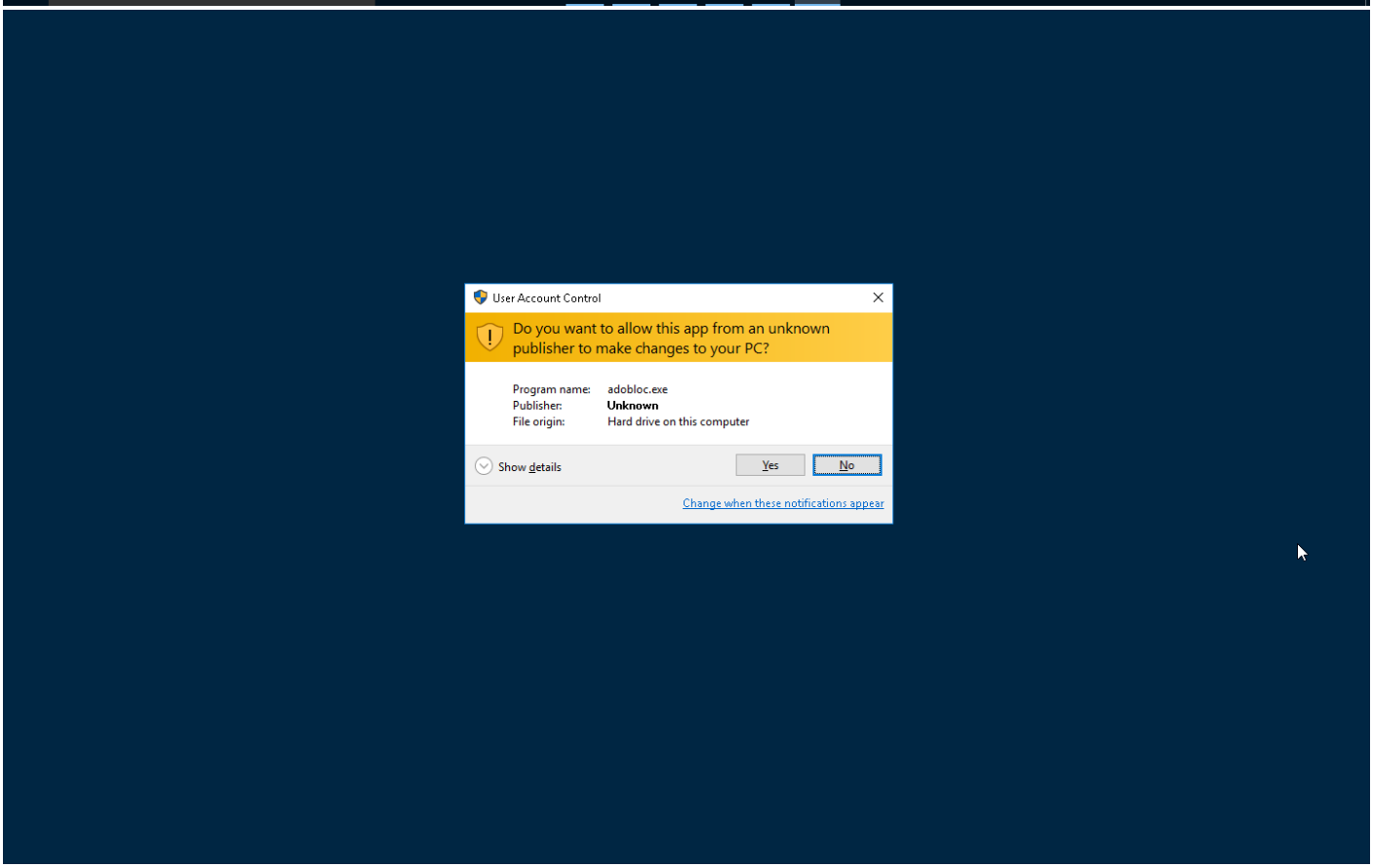
Sample Information

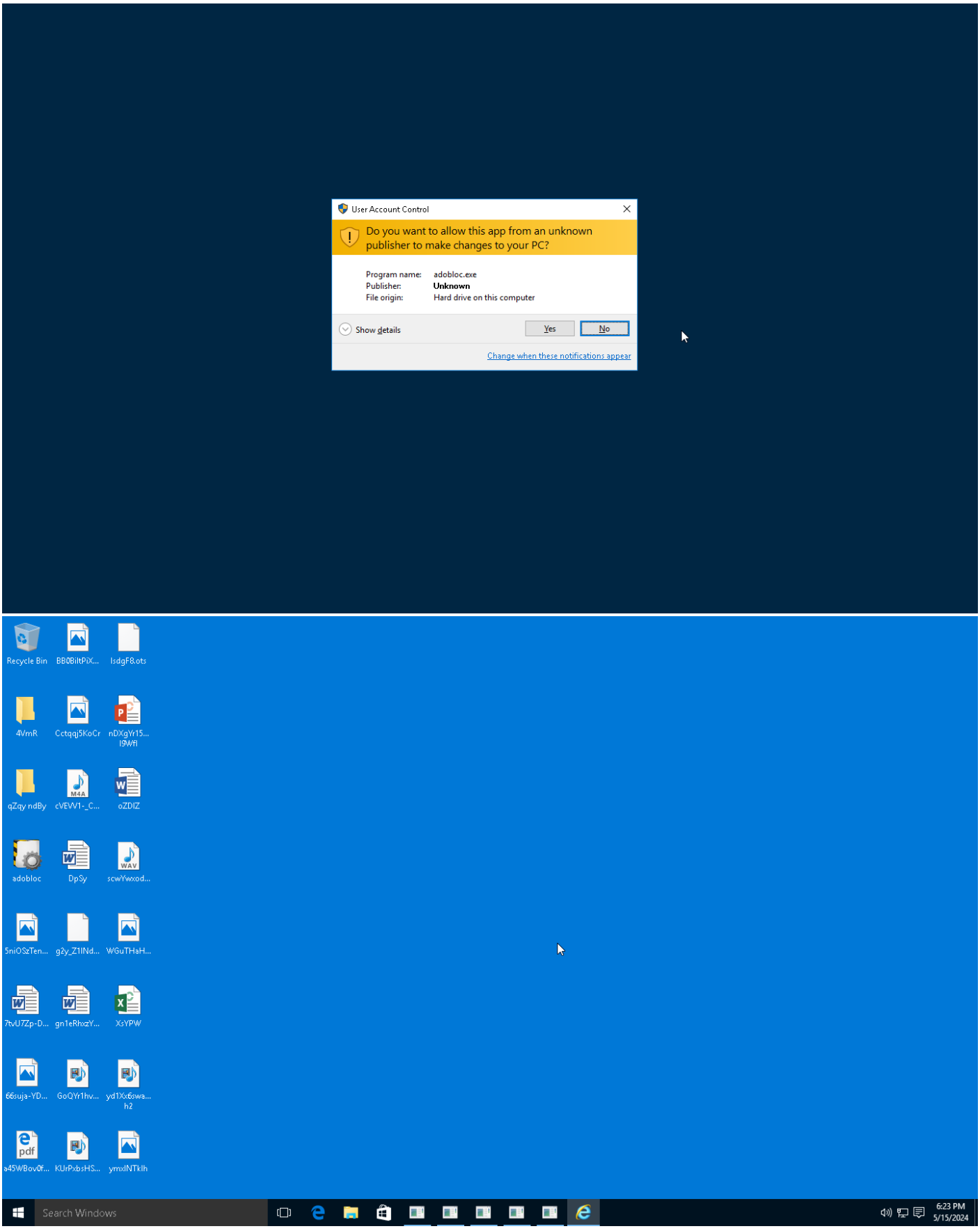
ID	#10437895
MD5	261a56d36006f274a3def7e2b0acb9d4
SHA1	3c6658e71b4b3a9c2200cf4c5cb337e1ebf449f4
SHA256	3e52c075a8eca95630727281a1380b78ac5392a035aef34aa3761afd1348e9f1
SSDeep	98304:+R0pl/lQlUoMPdmpSpM4ADtnkgvNWIw6aTfN41v:+R0plAQhMPdmn5n9klRKN41v
ImpHash	1a611a7df1f3828b0157c4725145a721
File Name	adobloc.exe
File Size	4218.89 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-05-15 20:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	36
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
BB0BiltPiX...
IsdgF8.ots
4VmR
Cctqqj5KoCr
nDXgYr15...
I9WFI
qZqy ndBy
cVEVV1-_C...
oZDIZ
adobloc
DpSy
scwYwxod...
5niOSzTen...
g2y_Z1INd...
WGuTHaH...
7tvU7Zp-D...
gn1eRhxzY...
XsYPW
66suja-YD...
GoQYr1hv...
yd1Xx6swa...
h2
a45WBov0f...
KUrPxbsHS...
ymxlNTklh
Search Windows
6:22 PM
5/15/2024


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



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

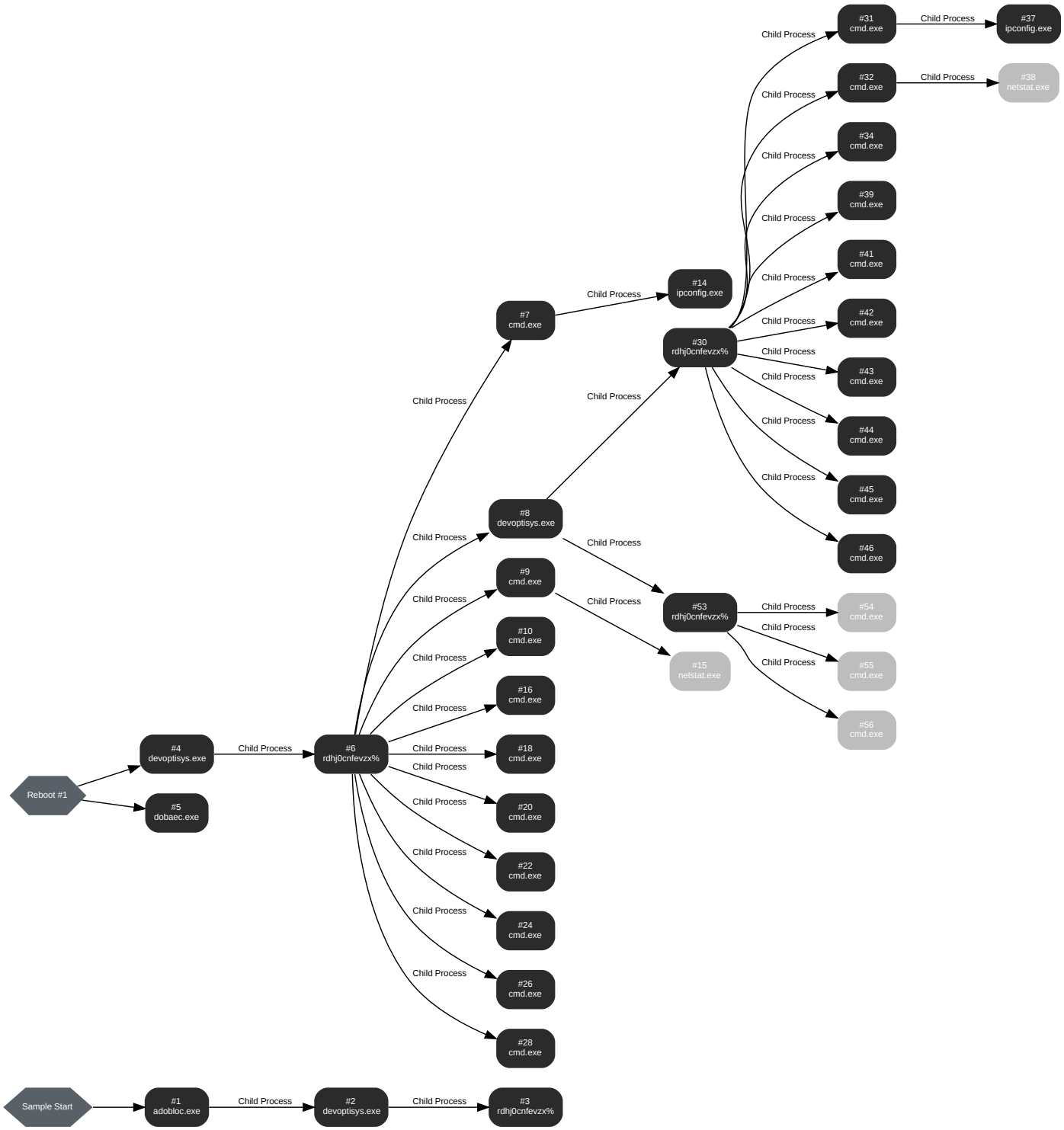
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: adobloc.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\adobloc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\adobloc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86084, Reason: Analysis Target
Unmonitor End Time	End Time: 127492, Reason: Terminated
Monitor duration	41.41s
Return Code	1073807364
PID	3476
Parent PID	-
Bitness	32 Bit

Dropped Files (8)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	216 bytes	4a4d3e0fbbae1b2fbfc23dfc7fba7baab479ed603505d3a27440c93ced0854d6	✖
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	213 bytes	3411d0be81cc9ea180def3521a01715d26ddba2294a9b87c905518f575d692c1	✖
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	216 bytes	8a0ee73a80d4f8ee24928369c4107c92c1fedc80adc80e569489f6f46b453148	✖
C:\KaVBJI\dobaec.exe	4218.95 KB	536b2aa3855bdb0df4491c48b29dc784e3d1fb736ef57d85a758006a20b791b1	✖
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	216 bytes	b29e3880621abec3d1a0707a917576ee09495b7b5633b9a26832dfd664a3cb00	✖
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	235 bytes	91e46da198cf5e6c13fd7c944367d0faf8d0add51d19411f889c60714bab640c	✖
C:\IntelprocSB\devoptisys.exe	4218.91 KB	61ecf0519833fdcccf07650287661dbb156cabed257dbbb64a72b428ce8af5c1	✖
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	235 bytes	ee30c8689c85917a525488ab7002d2179866ba1f8c7c8c7b994a4d86bb690c92	✖

Host Behavior

Type	Count
Module	120
File	555
System	1651
-	3
User	1
Registry	48
Process	848
Window	5

Process #2: devoptisys.exe

ID	2
File Name	c:\intelprocsb\devoptisys.exe
Command Line	C:\IntelprocSB\devoptisys.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103161, Reason: Child Process
Unmonitor End Time	End Time: 127477, Reason: Terminated
Monitor duration	24.32s
Return Code	1073807364
PID	2376
Parent PID	3476
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX%	4218.93 KB	1bbc7f0b18f31285ff33c570e8122400d3a0cd11bb0c99f5964f7afb49ebc2ba	✖

Host Behavior

Type	Count
Module	120
File	536
System	277
-	3
User	1
Registry	18
Process	316
Window	5

Process #3: rdhj0cnfevzx%

ID	3
File Name	c:\users\rdhj0cnfevzx%
Command Line	C:\Users\RDhJ0CNFevzX%
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115150, Reason: Child Process
Unmonitor End Time	End Time: 127461, Reason: Terminated
Monitor duration	12.31s
Return Code	1073807364
PID	928
Parent PID	2376
Bitness	32 Bit

Host Behavior

Type	Count
Module	122
File	289
System	132
-	3
User	1
Registry	5
Process	107
Window	5

Process #4: devoptisys.exe

ID	4
File Name	c:\intelprocsb\devoptisys.exe
Command Line	"C:\IntelprocSB\devoptisys.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 192270, Reason: Autostart
Unmonitor End Time	End Time: 219703, Reason: Terminated
Monitor duration	27.43s
Return Code	0
PID	2344
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	120
File	17
System	230
-	3
User	1
Registry	12
Process	70
Window	5

Process #5: dobaec.exe

ID	5
File Name	c:\kavbji\dobaec.exe
Command Line	"C:\KaVBJI\dobaec.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 193037, Reason: Autostart
Unmonitor End Time	End Time: 213436, Reason: Terminated
Monitor duration	20.40s
Return Code	0
PID	2468
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	120
File	17
System	254
-	3
User	1
Registry	12
Process	69
Window	5

Process #6: rdhj0cnfevzx%

ID	6
File Name	c:\users\rdhj0cnfevzx%
Command Line	C:\Users\RDhJ0CNFevzX%
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 211058, Reason: Child Process
Unmonitor End Time	End Time: 250251, Reason: Terminated
Monitor duration	39.19s
Return Code	217
PID	1180
Parent PID	2344
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\grubb.list	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	137
File	312
System	1709
-	3
User	1
Registry	48
Process	321
Window	5
Environment	1

Process #7: cmd.exe

ID	7
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220662, Reason: Child Process
Unmonitor End Time	End Time: 231949, Reason: Terminated
Monitor duration	11.29s
Return Code	0
PID	2892
Parent PID	1180
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\ipconfig.txt	775 bytes	bf503e0f96fff818da5c61fc6446c8613d294f16c3c69023ab6ca8723039c5cb	✖

Host Behavior

Type	Count
Module	1
File	12
Environment	8
Process	1

Process #8: devoptisys.exe

ID	8
File Name	c:\intelprocsb\devoptisys.exe
Command Line	C:\IntelprocSB\devoptisys.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220719, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	106.02s
Return Code	Unknown
PID	2608
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	122
File	269
System	6762
-	3
User	1
Registry	168
Process	1171
Window	5

Process #9: cmd.exe

ID	9
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 220873, Reason: Child Process
Unmonitor End Time	End Time: 243252, Reason: Terminated
Monitor duration	22.38s
Return Code	0
PID	724
Parent PID	1180
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\netstat.txt	1.78 KB	2cd15e7cc01bfa633f0db4388c104b1ab81706fc20d96aa798e4ee698090267d	✖

Host Behavior

Type	Count
Module	1
File	12
Environment	8
Process	1

Process #10: cmd.exe

ID	10
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 221068, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	105.67s
Return Code	Unknown
PID	656
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	6110
Environment	1

Process #14: ipconfig.exe

ID	14
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 227091, Reason: Child Process
Unmonitor End Time	End Time: 229976, Reason: Terminated
Monitor duration	2.88s
Return Code	0
PID	2676
Parent PID	2892
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	47
Environment	16
System	2

Process #15: netstat.exe

ID	15
File Name	c:\windows\syswow64\netstat.exe
Command Line	netstat -a
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 227247, Reason: Child Process
Unmonitor End Time	End Time: 242034, Reason: Terminated
Monitor duration	14.79s
Return Code	0
PID	2772
Parent PID	724
Bitness	32 Bit

Process #16: cmd.exe

ID	16
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 231685, Reason: Child Process
Unmonitor End Time	End Time: 238421, Reason: Terminated
Monitor duration	6.74s
Return Code	1
PID	2936
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #18: cmd.exe

ID	18
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 242149, Reason: Child Process
Unmonitor End Time	End Time: 252681, Reason: Terminated
Monitor duration	10.53s
Return Code	1
PID	3052
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #20: cmd.exe

ID	20
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 243408, Reason: Child Process
Unmonitor End Time	End Time: 252305, Reason: Terminated
Monitor duration	8.90s
Return Code	1
PID	1676
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #22: cmd.exe

ID	22
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 244698, Reason: Child Process
Unmonitor End Time	End Time: 253722, Reason: Terminated
Monitor duration	9.02s
Return Code	1
PID	2328
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #24: cmd.exe

ID	24
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 245952, Reason: Child Process
Unmonitor End Time	End Time: 254309, Reason: Terminated
Monitor duration	8.36s
Return Code	1
PID	1572
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #26: cmd.exe

ID	26
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 247173, Reason: Child Process
Unmonitor End Time	End Time: 254628, Reason: Terminated
Monitor duration	7.46s
Return Code	1
PID	2260
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #28: cmd.exe

ID	28
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 247660, Reason: Child Process
Unmonitor End Time	End Time: 254935, Reason: Terminated
Monitor duration	7.28s
Return Code	1
PID	1980
Parent PID	1180
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #30: rdhj0cnfevzx%

ID	30
File Name	c:\users\rdhj0cnfevzx%
Command Line	C:\Users\RDhJ0CNFevzX%
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 252133, Reason: Child Process
Unmonitor End Time	End Time: 301298, Reason: Terminated
Monitor duration	49.16s
Return Code	217
PID	2556
Parent PID	2608
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\oZDlZ.docx.exe	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	146
File	602
System	3625
-	3
User	1
Registry	84
Process	567
Window	5
Environment	1

Process #31: cmd.exe

ID	31
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 271708, Reason: Child Process
Unmonitor End Time	End Time: 279565, Reason: Terminated
Monitor duration	7.86s
Return Code	0
PID	1552
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	12
Environment	8
Process	1

Process #32: cmd.exe

ID	32
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 271946, Reason: Child Process
Unmonitor End Time	End Time: 296459, Reason: Terminated
Monitor duration	24.51s
Return Code	0
PID	2612
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	12
Environment	8
Process	1

Process #34: cmd.exe

ID	34
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 272189, Reason: Child Process
Unmonitor End Time	End Time: 278571, Reason: Terminated
Monitor duration	6.38s
Return Code	1
PID	816
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #37: ipconfig.exe

ID	37
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 275726, Reason: Child Process
Unmonitor End Time	End Time: 277274, Reason: Terminated
Monitor duration	1.55s
Return Code	0
PID	764
Parent PID	1552
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	47
Environment	16
System	2

Process #38: netstat.exe

ID	38
File Name	c:\windows\syswow64\netstat.exe
Command Line	netstat -a
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 276378, Reason: Child Process
Unmonitor End Time	End Time: 293201, Reason: Terminated
Monitor duration	16.82s
Return Code	0
PID	724
Parent PID	2612
Bitness	32 Bit

Process #39: cmd.exe

ID	39
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 282835, Reason: Child Process
Unmonitor End Time	End Time: 297941, Reason: Terminated
Monitor duration	15.11s
Return Code	1
PID	780
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #41: cmd.exe

ID	41
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 293202, Reason: Child Process
Unmonitor End Time	End Time: 308465, Reason: Terminated
Monitor duration	15.26s
Return Code	1
PID	1524
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #42: cmd.exe

ID	42
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 293887, Reason: Child Process
Unmonitor End Time	End Time: 309392, Reason: Terminated
Monitor duration	15.51s
Return Code	1
PID	1572
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #43: cmd.exe

ID	43
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 294647, Reason: Child Process
Unmonitor End Time	End Time: 308465, Reason: Terminated
Monitor duration	13.82s
Return Code	1
PID	2720
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #44: cmd.exe

ID	44
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 295796, Reason: Child Process
Unmonitor End Time	End Time: 310504, Reason: Terminated
Monitor duration	14.71s
Return Code	1
PID	2260
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #45: cmd.exe

ID	45
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 296921, Reason: Child Process
Unmonitor End Time	End Time: 310497, Reason: Terminated
Monitor duration	13.58s
Return Code	1
PID	3016
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #46: cmd.exe

ID	46
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir Z:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 297653, Reason: Child Process
Unmonitor End Time	End Time: 310959, Reason: Terminated
Monitor duration	13.31s
Return Code	1
PID	2692
Parent PID	2556
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	15

Process #53: rdhj0cnfevzx%

ID	53
File Name	c:\users\rdhj0cnfevzx%
Command Line	C:\Users\RDhJ0CNFevzX%
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 302471, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	24.27s
Return Code	Unknown
PID	2316
Parent PID	2608
Bitness	32 Bit

Host Behavior

Type	Count
Module	128
File	302
System	951
-	3
User	1
Registry	24
Process	160
Window	5

Process #54: cmd.exe

ID	54
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 322288, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	4.45s
Return Code	Unknown
PID	1108
Parent PID	2316
Bitness	32 Bit

Process #55: cmd.exe

ID	55
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 322467, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	4.27s
Return Code	Unknown
PID	2872
Parent PID	2316
Bitness	32 Bit

Process #56: cmd.exe

ID	56
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 322781, Reason: Child Process
Unmonitor End Time	End Time: 326740, Reason: Terminated by timeout
Monitor duration	3.96s
Return Code	Unknown
PID	1500
Parent PID	2316
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3e52c075a8eca95630727281a1380b78ac5392a035aef34aa3761afd1348e9f1	C:\Users\RDhJ0CNFevzX\Desktop\adobloc.exe	Sample File	4218.89 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
1bbc7f0b18f31285ff33c570e8122400d3a0cd11bb0c99f5964f7afb49ebc2ba	C:\Users\RDhJ0CNFevzX%	Dropped File	4218.93 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
7ee27d6d1cb9dd888a3a5a557b298d3eae41f24c5ba3b0b32a8080065f1b5428	-	Extracted File	376 bytes	image/png	-	CLEAN
1714c78207dc35876976b442ca8f89d6abd79962e35ddc661d2e39a443488342	-	Extracted File	512 bytes	image/png	-	CLEAN
214ccdf39043a8af0bdc8321ca3015bb57fafbde737a7a2440f5d6f6843458ab	-	Extracted File	584 bytes	image/png	-	CLEAN
8deca71c2daf7bb420244740748e86446b307af93a9c3ee2a13d1bc082b33a10	-	Extracted File	633 bytes	image/png	-	CLEAN
e106f7f299d78e4dca40450883bb093f7cd1378d53983b867b7cef9993bd02f8	-	Extracted File	838 bytes	image/png	-	CLEAN
c7055a97d4bf7b106f58c00070a22b1d09082344cf40685f98f8d1c433327a0c	-	Extracted File	876 bytes	image/png	-	CLEAN
984bbca1cc2a014b08b9f4a8fd8ee9068c3f4f23b77730ededb08cb9da7fda42	-	Extracted File	489 bytes	image/png	-	CLEAN
da2fa5885361bf6dec84d6d406485acb0d6775bcd7b80321f00c73a1cd4f0cc2	-	Extracted File	579 bytes	image/png	-	CLEAN
4fc8467a6cee88ea4399139aede19a67b3fb8a709f260de13508a47409e0da69	-	Extracted File	789 bytes	image/png	-	CLEAN
3469503fc64c55815809de519c47ab160a5a99d4c18caa743b4384ee0a724ae6	-	Extracted File	550 bytes	image/png	-	CLEAN
19a618dad57c410b9c3abc6b440f02c5f2216a913eed8d3365a41c094d069f5e	-	Extracted File	745 bytes	image/png	-	CLEAN
0ccb16682f13a75b29a8e19d71cc2b33eb8bbd7ce04a8871a06a791f269c943b	-	Extracted File	925 bytes	image/png	-	CLEAN
63113b2d9cdf6daebdf9b8e6207983a09ab70a2f95140f2acc7bb4c7484577c9	-	Extracted File	730 bytes	image/png	-	CLEAN
18e20847b3a4ce78202efc0da5d396028e6bddf8a7cbe47877172c50c26b4a6e	-	Extracted File	1.06 KB	image/png	-	CLEAN
e75d2f5b882d37aad4a527ff7727d9e7645c57b02e7a4fe47651db0571672235	-	Extracted File	1.40 KB	image/png	-	CLEAN
b91661b56ba60fd88d0436280b0b319aaf4a741ec715873bd0b50f126f17bef7	-	Extracted File	612 bytes	image/png	-	CLEAN
5787581fc804c120df743e12098f08ce58b272006253a06d5fbb4076541d97ae	-	Extracted File	865 bytes	image/png	-	CLEAN
e8083d39b49e33edb47eff8fcafa5a5507a5e5a4c558c6b1e151b1d27f1aa2e8	-	Extracted File	1.17 KB	image/png	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a2bcef8d11e19e0cd18e2920871c294e4007a603cee95b29511579171515d9fe	-	Extracted File	620 bytes	image/png	-	CLEAN
e9aee2a7155c4de9910decbf5b27c255d82d0c39e0ebc3baa365944fc376c376	-	Extracted File	960 bytes	image/png	-	CLEAN
f185f322e2041074006f7b816914afda83fa7e90265490bf3fe1c24a11e62176	-	Extracted File	1.30 KB	image/png	-	CLEAN
2af5eb4a28229e28e77d4850a7e96ad7bddf8a3ac5dbcede469b1be2505182ba	-	Extracted File	461 bytes	image/png	-	CLEAN
84f0654345776a6ca545dd69990e34d06020012ccca8b402fda87b5b1428eb82	-	Extracted File	684 bytes	image/png	-	CLEAN
77d24a01ad76c86290bb45b9bd614621f3d66c8da9ded252c181bfefacf277f6	-	Extracted File	804 bytes	image/png	-	CLEAN
099125b54dbc4290932166f8833c62050782e085db727094f378b659d9df9fbf	-	Extracted File	893 bytes	image/png	-	CLEAN
4a24971851c42fb80e201a33239dc4573b65a922bb90653b23bb344c4eb6b878	-	Extracted File	1.33 KB	image/png	-	CLEAN
98448c1a43b72867ac08344f25e5faa5b55dbfb474c0adb91de05efa034c03c1	-	Extracted File	1.55 KB	image/png	-	CLEAN
842914e746afd743c0b4319b2ccb1d80f1e88ec1c162cbd70112d81e68f7c5c0	-	Extracted File	2.03 KB	image/png	-	CLEAN
b965e37e3bb998029faf25df2fa9bef5b3c4e4f7d52054e1b707c1b1cc1d5ed1	-	Extracted File	1.50 KB	image/png	-	CLEAN
a0a1b573a6b491299c13d2728ee7bd0ea9417ab35183eefe55cca090ffd535c3	-	Extracted File	1.78 KB	image/png	-	CLEAN
b8748c0322852287a898da843a4dea7d581151ae42aa920fcd6eed2c69d098cc	-	Extracted File	1.77 KB	image/png	-	CLEAN
408da8e699df3b28f178859773ef0a3bae5bb98e6359a37335b71efcea534fed	-	Extracted File	1.27 KB	image/png	-	CLEAN
5fca6f0494825f91674d7b0991fed54d37656318b5438119ef14abe942a4568e	-	Extracted File	367 bytes	image/png	-	CLEAN
e43fa1c7c8d01e8f09c09a6ebac6b07bdd8b5f732f422e3e1458b1f248af3872	-	Extracted File	404 bytes	image/png	-	CLEAN
5337cd89b2f10858d9e0737dc9b4508a91f53698e2ae9c0b71b37434cb0f285f	-	Extracted File	579 bytes	image/png	-	CLEAN
828552b82b42ce737cc387976880aad36629bf16d63c029153a0cbeec0d6a05b	-	Extracted File	264 bytes	image/png	-	CLEAN
84ca1578ef156a0bc84cb9d9d5d176620109b231dda4ba244450eaf6055f0857	-	Extracted File	354 bytes	image/png	-	CLEAN
3dbd71020e4826cd755c9cdfdf04b21be018543f35d6e9451ff06b488e675782	-	Extracted File	381 bytes	image/png	-	CLEAN
777ca72dc7a8b663b47156656cc736a7e895a2905d88c18cc7c9644fbddac237	-	Extracted File	433 bytes	image/png	-	CLEAN
9275ef0f309be9754a5586f730cb3164bd9a81351dd34db4ed0896fd046556a7	-	Extracted File	575 bytes	image/png	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
eca821a2347305c0f5e3f3526026b23bdcbcdae775c84726140b446b3bef83f7	-	Extracted File	301 bytes	image/png	-	CLEAN
6002ad2939e01c4213afa5139a59e7d5ade74a3f23c9631e5048e5c17047e254	-	Extracted File	349 bytes	image/png	-	CLEAN
3411d0be81cc9ea180def3521a01715d26ddba2294a9b87c905518f575d692c1	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	213 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN
61ecf0519833fdcccf07650287661dbb156cabed257dbbb64a72b428ce8af5c1	C:\IntelprocSB\devoptisys.exe	Dropped File	4218.91 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	CLEAN
8a0ee73a80d4f8ee24928369c4107c92c1fedc80adc80e569489f6f46b453148	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	216 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN
4a4d3e0fbbae1b2fbfc23dfc7fba7baab479ed603505d3a27440c93ced0854d6	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	216 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN
536b2aa3855bdb0df4491c48b29dc784e3d1fb736ef57d85a758006a20b791b1	C:\KaVBJI\dobaec.exe	Dropped File	4218.95 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	CLEAN
b29e3880621abec3d1a0707a917576ee09495b7b5633b9a26832dfd664a3cb00	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	216 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN
bf503e0f96fff818da5c61fc6446c8613d294f16c3c69023ab6ca8723039c5cb	C:\Users\RDhJ0CNFevzX\ipconfig.txt	Dropped File	775 bytes	text/plain	Access, Create	CLEAN
2cd15e7cc01bfa633f0db4388c104b1ab81706fc20d96aa798e4ee698090267d	C:\Users\RDhJ0CNFevzX\netstat.txt	Dropped File	1.78 KB	text/plain	Access, Create	CLEAN
ee30c8689c85917a525488ab7002d2179866ba1f8c7c8c7b994a4d86bb690c92	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	235 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN
91e46da198cf5e6c13fd7c944367d0faf8d0add51d19411f889c60714bab640c	C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Dropped File	235 bytes	application/x-wine-extension-ini	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\adobloc.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\oZDlZ.docx.exe	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\549752664064_10.0_RDhJ0CNFevzX.ini	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\IntelprocSB\devoptisys.exe	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX%	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\KaVBJI\dobaec.exe	Accessed File, Dropped File, Modified File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\grubb.list	Accessed File, Dropped File, Modified File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\grubb.dan	Accessed File, Dropped File, Modified File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\ipconfig.txt	Accessed File, Dropped File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\netstat.txt	Accessed File, Dropped File	Access, Create	CLEAN
C:\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX% 99 *=*%8*6270%2,;8<8/=%27-8@<%=*;=.7>%;80;*6<%=*;=>9%locabod.exe	Accessed File	Access	CLEAN
C:\IntelprocSB	Accessed File	Access, Create	CLEAN

File Name	Category	Operations	Verdict
C:\KaVBJI	Accessed File	Access, Create	CLEAN
C:*.txt	Accessed File	Access	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	create, access	rdhj0cnfevzx%, dobaec.exe, adobloc.exe, devoptisys.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Parametr	access, read, write	rdhj0cnfevzx%, dobaec.exe, adobloc.exe, devoptisys.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	create, access	rdhj0cnfevzx%, dobaec.exe, adobloc.exe, devoptisys.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Parametr	access, read, write	rdhj0cnfevzx%, dobaec.exe, adobloc.exe, devoptisys.exe	CLEAN

Process

Process Name	Commandline	Verdict
rdhj0cnfevzx%	C:\Users\RDhJ0CNFevzX%	MALICIOUS
adobloc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\adobloc.exe"	MALICIOUS
ipconfig.exe	ipconfig	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	SUSPICIOUS
ipconfig.exe	ipconfig	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
netstat.exe	netstat -a	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir Z:*.rtf /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
rdhj0cnfevzx%	C:\Users\RDhJ0CNFevzX%	CLEAN
devoptisys.exe	C:\IntelprocSB\devoptisys.exe	CLEAN
rdhj0cnfevzx%	C:\Users\RDhJ0CNFevzX%	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt	CLEAN

Process Name	Commandline	Verdict
cmd.exe	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.txt /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
devoptisys.exe	"C:\IntelprocSB\devoptisys.exe"	CLEAN
dobaec.exe	"C:\KaVBJI\dobaec.exe"	CLEAN
rdhj0cnfevzx%	C:\Users\RDhJ0CNFevzX%	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c ipconfig > C:\Users\RDhJ0CNFevzX\ipconfig.txt	CLEAN
devoptisys.exe	C:\IntelprocSB\devoptisys.exe	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c netstat -a > C:\Users\RDhJ0CNFevzX\netstat.txt	CLEAN
netstat.exe	netstat -a	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.doc /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c dir C:*.xls /b /s >> C:\Users\RDhJ0CNFevzX\grubb.list	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.29 / 2024-05-11 04:28:14
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.27 / 2024-05-02 14:06:04
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.29 / 2024-05-11 04:28:14
YARA Built-in Ruleset Version	2024.2.1.24

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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows