MALICIOUS

Classifications: Ransomware

Threat Names: Sodinokibi

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Avaddon_09_06_2020_1054KB.exe**
ID	#3193061
MD5	c9ec0d9ff44f445ce5614cc87398b38d
SHA1	591ffe54bac2c50af61737a28749ff8435168182
SHA256	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
File Size	1053.50 KB
Report Created	2021-12-27 19:14 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 67 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 26 files by appending the extension ".avdn".			
5/5	User Data Modification	Modifies Windows automatic backups	1	-
	• (Process #1) avaddon_09_06_2020_1054kb.exe deletes Windows volume shadow copies.			
5/5	YARA	Malicious content matched by YARA rules	24	Ransomware
	• Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Contacts\Administrator.contact". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSN Autos.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSN Entertainment.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSN Money.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSN Sports.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSN.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Favorites\MSN Websites\MSNBC News.url". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\NTUSER.DAT.LOG". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\NTUSER.DAT.LOG1". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\NTUSER.DAT.LOG2". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Searches\Everywhere.search-ms". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\Default\Searches\Indexed Locations.search-ms". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\-Czpv.mp3". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\-ozBRluaHqu9LIfa7.flv". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\05Gh.mkv". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe 59.mp3". • Rule "SodinokibiEncryptedFile" from ruleset "Ransomware" has matched on the modified file "C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7I.wav".			
5/5	User Data Modification	Encrypts content of user files	1	Ransomware
	• (Process #1) avaddon_09_06_2020_1054kb.exe encrypts the content of multiple user files.			
4/5	Defense Evasion	Bypasses Windows User Account Control (UAC)	1	-
	• (Process #1) avaddon_09_06_2020_1054kb.exe disables UAC dialog via registry.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	Discovery	Reads SMB connection information	27	-

Score	Category	Operation	Count	Classification
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "A:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "B:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "C:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "D:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "E:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "F:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "G:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "H:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "I:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "J:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "K:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "L:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "M:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "N:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "O:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "P:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "Q:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "R:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "S:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "T:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "U:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "V:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "W:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "X:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "Y:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "Z:".		
		• (Process #1) avaddon_09_06_2020_1054kb.exe collects information on network shares at "192.168.0.1".		
2/5	Anti Analysis	Tries to detect debugger	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe tries to detect a debugger via API "IsDebuggerPresent".		
2/5	Data Collection	Reads sensitive application data	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe tries to read sensitive data of application "git" by file.		
2/5	Data Collection	Reads sensitive ftp data	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe tries to read sensitive data of ftp application "Total Commander" by file.		
2/5	Task Scheduling	Schedules task	1	-
		• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\Avaddon_09_06_2020_1054KB.exe", to be triggered by Calendar. Task has been rescheduled by the analyzer.		
1/5	Mutex	Creates mutex	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe creates mutex with name "{2A0E9C7B-6BE8-4306-9F73-1057003F605B}".		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe adds "C:\Users\kEecfMwgj\AppData\Roaming\Avaddon_09_06_2020_1054KB.exe" to Windows startup via registry.		
1/5	Discovery	Enumerates running processes	1	-
		• (Process #1) avaddon_09_06_2020_1054kb.exe enumerates running processes.		

Score	Category	Operation	Count	Classification
1/5	Privilege Escalation	Enables process privilege	3	-
	• (Process #3) wmic.exe enables process privilege "". • (Process #9) wmic.exe enables process privilege "". • (Process #11) wmic.exe enables process privilege "".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) avaddon_09_06_2020_1054kb.exe resolves 48 API functions by name.			

Mitre ATT&CK Matrix

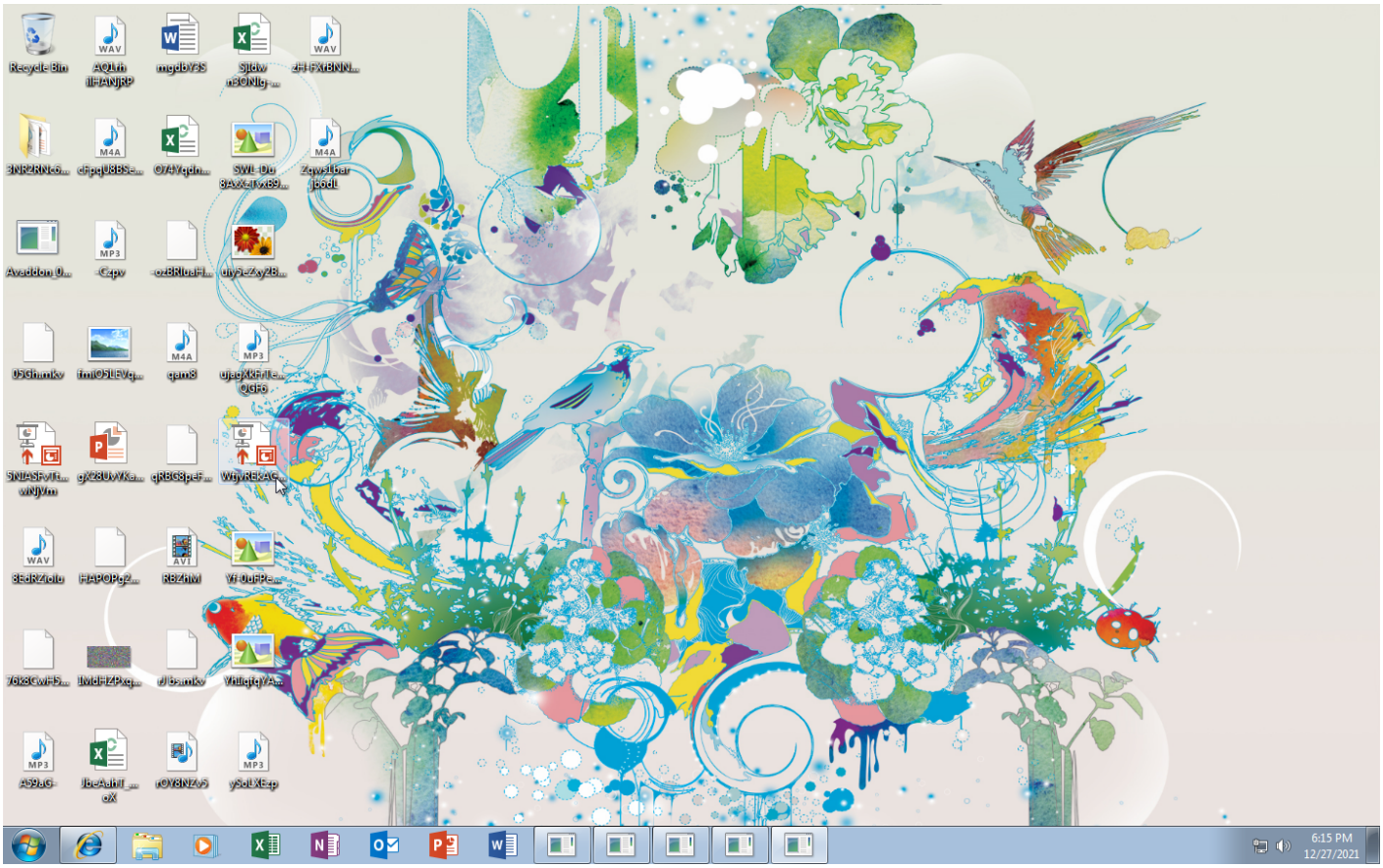
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1112 Modify Registry	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
		#T1053 Scheduled Task		#T1045 Software Packing		#T1049 System Network Connections Discovery		#T1005 Data from Local System			#T1490 Inhibit System Recovery
						#T1135 Network Share Discovery					
						#T1057 Process Discovery					
						#T1083 File and Directory Discovery					

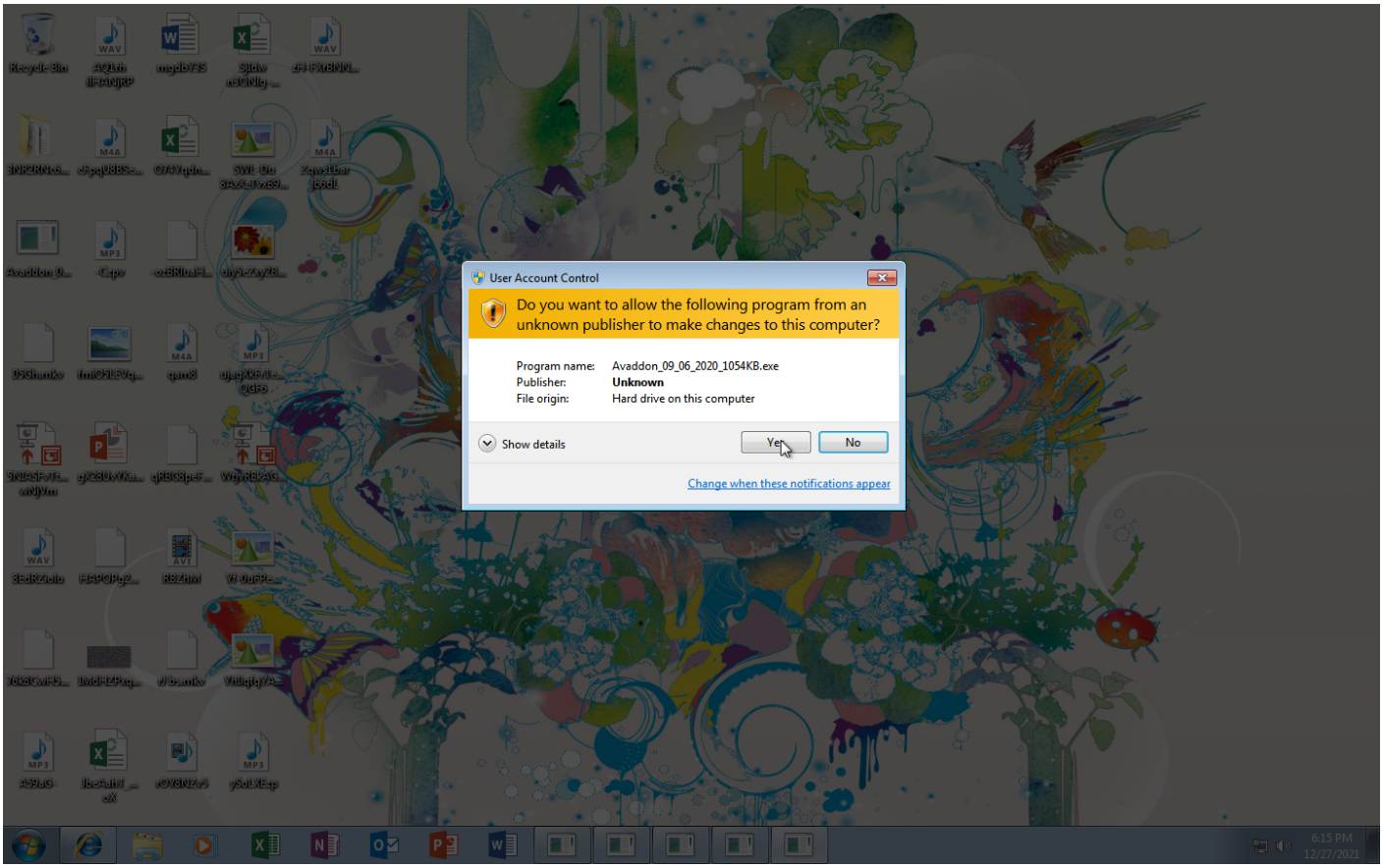
Sample Information

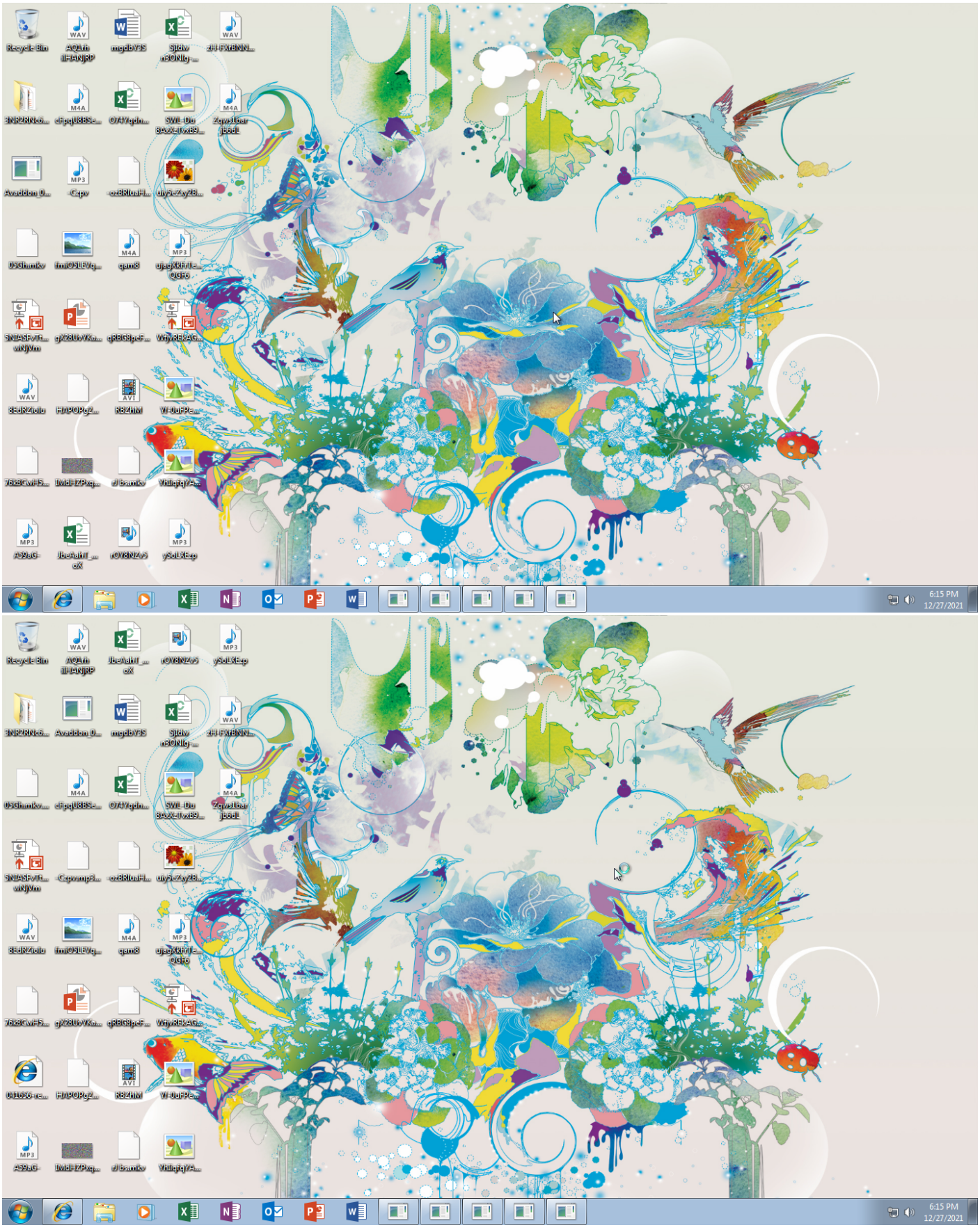
ID	#3193061
MD5	c9ec0d9ff44f445ce5614cc87398b38d
SHA1	591ffe54bac2c50af61737a28749ff8435168182
SHA256	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
SSDeep	24576:Cs6JmdFn5KLOCgHWcAvcrOcEsKfR9uA7rmFbbbbpccf:Cs6JY5KLOCyWcDUfRAA3mFbbbbpc4
ImpHash	1156e59d43883136ef73eee451e94e3d
File Name	Avaddon_09_06_2020_1054KB.exe
File Size	1053.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-12-27 19:14 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	24




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: Avaddon_09_06_2020_1054KB.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

816 bytes total sent

5.39 KB total received

1 ports 443

2 contacted IP addresses

1 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

1 URLs contacted, 1 servers

1 sessions, 816 bytes sent, 5.39 KB received

HTTP Requests

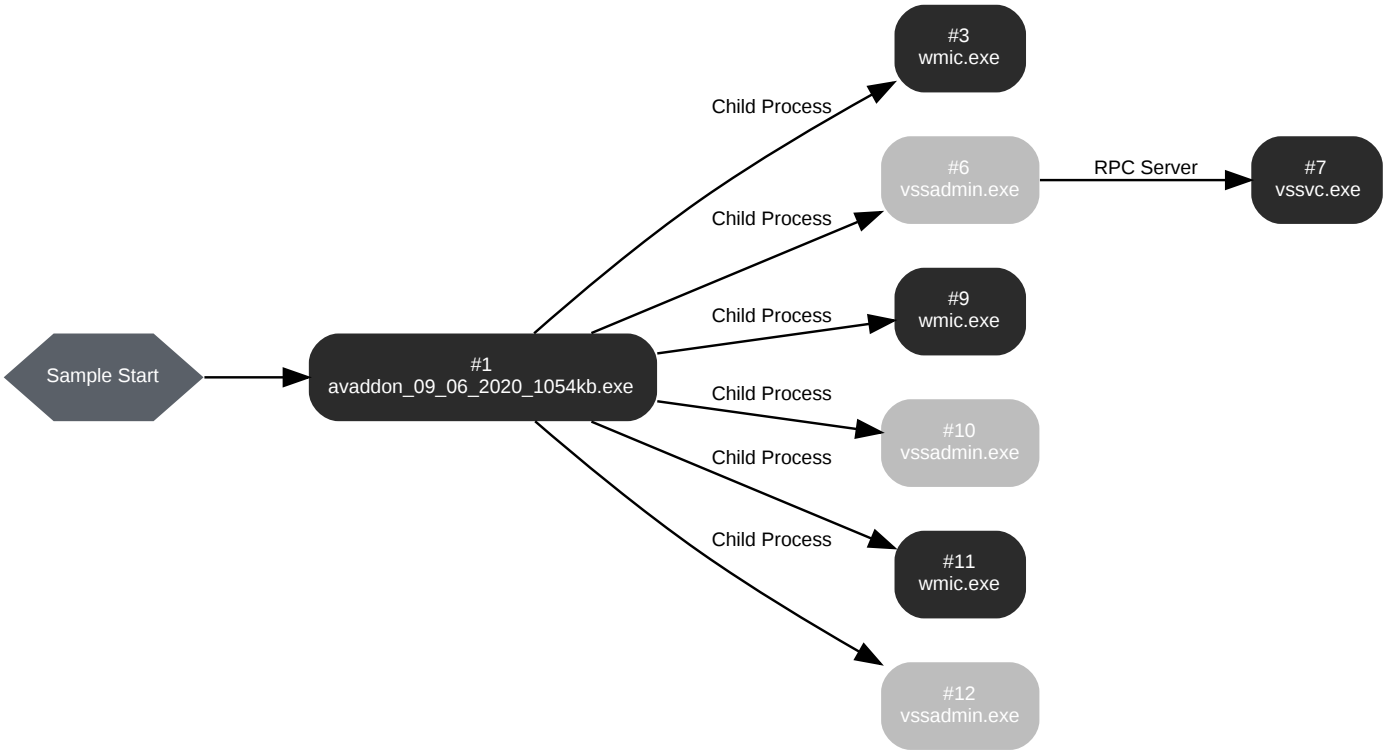
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://api.myip.com	-	-		0 bytes	NA
GET	https://www.torproject.org/	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
-	q9iatrkprh	-	192.168.0.129		NA

BEHAVIOR

Process Graph



Process #1: avaddon_09_06_2020_1054kb.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\avaddon_09_06_2020_1054kb.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\Avaddon_09_06_2020_1054KB.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 56815, Reason: Analysis Target
Unmonitor End Time	End Time: 113597, Reason: Terminated
Monitor duration	56.78s
Return Code	1073807364
PID	2788
Parent PID	912
Bitness	32 Bit

Dropped Files (29)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\Avaddon_09_06_2020_1054KB.exe	1053.50 KB	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2	✗
-	50 bytes	2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	✗
C:\Users\Default\Contacts\Administrator.contact	72.52 KB	d9ecb29f3ef3f7d967c6c6118cda547b5bb9c99b45294b5979e2ab7aa694109a	✗
C:\Users\Default\Contacts\041656-readme.html	49.89 KB	e6327db35ddc7e174a160187944432f8ea2da6283c4bbeb96e2e50491b694412	✗
C:\Users\Default\Favorites\Links\Web Slice Gallery.url	8.52 KB	d04199b8d17f90a3663a721add9b20f4d1f07d8f4714e45644cf3c38ce810fc4	✗
C:\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url	8.52 KB	257d60bf2fde40d0282bb05aeb69a0c350a82a03a96156b7d76c23441d2140d9	✗
C:\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url	8.52 KB	5a64312c449747496728127ca6ca53bbea2a7c883020a46db87aaf7b53d5c3f1	✗
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url	8.52 KB	e04f6b8910d36f6096d6afa4f57bd3d347a7810caa4ffe6773e20c5a047269c0	✗
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url	8.52 KB	192956dd8bc9fbd3819c47db66713e6fcc5fcaea3c0beedf8833067b6cb4780b	✗
C:\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url	8.52 KB	83567f9f7aba5b25d18788e4553a368f6620ec3e81982fb6e1acf07dd0fcdd72	✗
C:\Users\Default\Favorites\MSN Websites\MSN Autos.url	8.52 KB	7faa30db6ec952b6f101b4843ab04c2a1c5ca0ebcf5d8846ffdc0b5c2401b91d	✗
C:\Users\Default\Favorites\MSN Websites\MSN Entertainment.url	8.52 KB	a026e99e2b81985eaf24a559f7b94021e4678a89d4b6d9cdb465bff598d98e45	✗
C:\Users\Default\Favorites\MSN Websites\MSN Money.url	8.52 KB	921d4eb5eb76a3175ec4751ad417bbc50d828becfe375cd7b6a8c555267ea361	✗
C:\Users\Default\Favorites\MSN Websites\MSN Sports.url	8.52 KB	f098125e203baa7ab39f64487d8f4bd1563d16244c66e5cfa9d391dad952f6a3	✗
C:\Users\Default\Favorites\MSN Websites\MSN.url	8.52 KB	d65df7c29218553d712f4da24708790c7885796d4c7425ed1268c14e0c89248c	✗
C:\Users\Default\Favorites\MSN Websites\MSNBC News.url	8.52 KB	d9dfa3a6665b8bd39d0f0d3f80a3afc907d63e7d49c798b8e1504b225badd0f0	✗
C:\Users\Default\NTUSER.DAT.LOG	8.52 KB	ea49d66b62cfe879946ba63bfced7501c660c2ec03da7a3051765367fcba5546	✗
C:\Users\Default\NTUSER.DAT.LOG1	192.52 KB	d3be08dd25b5915e412c1132de55a2f330a358afb446cb926627b9b9b4788982	✗

File Name	File Size	SHA256	YARA Match
C:\\Users\Default\NTUSER.DAT.LOG2	536 bytes	57c69af0f317ccc0aa33cd947c31f9b02c8b0f833add27f9e5cc477771033302	✗
C:\\Users\Default\Searches\Everywhere.search-ms	8.52 KB	666045045b6042fcc9f374704a927943774577f52387b0183d618d348768f5a1	✗
C:\\Users\Default\Searches\Indexed Locations.search-ms	8.52 KB	0721be5c78a690aad8495b4ca997cba2f3b6626f6d389a69dd59dfe1993486ef	✗
C:\\Users\kEecfMwgj\Desktop\-Czpv.mp3	8.52 KB	13e398b5049ecb6db494eb9231bfc0de8e804e74b82a51837abffbf43a8f25a3	✗
C:\\Users\kEecfMwgj\Desktop\-ozBRIuaHqu9LIfa7.flv	40.52 KB	2f7215137d9585f448e8e51e6424ad1feb93b870a9683450fce796aa906da4f6	✗
C:\\Users\kEecfMwgj\Desktop\05Gh.mkv	48.52 KB	99c21e95839b9755fa2c23442f00d989812d6d71384f9e4ddba6d24019838d43	✗
C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps	72.52 KB	7a08f1c46d158cf559e79b4d5834328c84ff3c1ba831cf8bd87040ec82b75c95	✗
C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf	8.52 KB	155c3781ec3c88ec5be0243ed682b7ba578f05df47c7e869ecfa30281af9d9e4	✗
C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe59.mp3	8.52 KB	c8adffad1f7f529380208fa82c75535ead186b0e51c15f6dace5562452c21460	✗
C:\\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7l.wav	88.52 KB	47bdaf781b239e7ada8caa09ac1144e581c94eb1f47dd03eacc4a2f15c19942c	✗
-	208 bytes	6a4a2c79766c3189f448cf9e5466cf16bcad560680e5e5b2dc5fae580fca6da4	✗

Host Behavior

Type	Count
System	46
Module	97
File	434
Environment	3
-	1
Keyboard	1
Mutex	2
Process	276
Registry	10
COM	1
-	100
-	53

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	1

Process #3: wmic.exe

ID	3
File Name	c:\windows\syswow64\wbem\wmic.exe
Command Line	wmic.exe SHADOWCOPY /nointeractive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92777, Reason: Child Process
Unmonitor End Time	End Time: 97962, Reason: Terminated
Monitor duration	5.18s
Return Code	44124
PID	2564
Parent PID	2788
Bitness	32 Bit

Host Behavior

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

Process #6: vssadmin.exe

ID	6
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96799, Reason: Child Process
Unmonitor End Time	End Time: 99479, Reason: Terminated
Monitor duration	2.68s
Return Code	2
PID	548
Parent PID	2788
Bitness	32 Bit

Process #7: vssvc.exe

ID	7
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 98304, Reason: RPC Server
Unmonitor End Time	End Time: 296863, Reason: Terminated by Timeout
Monitor duration	198.56s
Return Code	Unknown
PID	552
Parent PID	456
Bitness	64 Bit

Host Behavior

Type	Count
System	3

Process #9: wmic.exe

ID	9
File Name	c:\windows\syswow64\wbem\wmic.exe
Command Line	wmic.exe SHADOWCOPY /nointeractive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98542, Reason: Child Process
Unmonitor End Time	End Time: 100858, Reason: Terminated
Monitor duration	2.32s
Return Code	44124
PID	2080
Parent PID	2788
Bitness	32 Bit

Host Behavior

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

Process #10: vssadmin.exe

ID	10
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99862, Reason: Child Process
Unmonitor End Time	End Time: 102155, Reason: Terminated
Monitor duration	2.29s
Return Code	2
PID	2488
Parent PID	2788
Bitness	32 Bit

Process #11: wmic.exe

ID	11
File Name	c:\windows\syswow64\wbem\wmic.exe
Command Line	wmic.exe SHADOWCOPY /nointeractive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 100126, Reason: Child Process
Unmonitor End Time	End Time: 102154, Reason: Terminated
Monitor duration	2.03s
Return Code	44124
PID	2916
Parent PID	2788
Bitness	32 Bit

Host Behavior

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

Process #12: vssadmin.exe

ID	12
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 100711, Reason: Child Process
Unmonitor End Time	End Time: 102154, Reason: Terminated
Monitor duration	1.44s
Return Code	2
PID	2896
Parent PID	2788
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d9ecb29f3ef3f7d967c6c6118cda547b5bb9c99b45294b5979e2ab7aa694109a	C:\\Users\kEecfMwgj\Contacts\Administrator.contact.avdn, C:\\Users\Default\Contacts\Administrator.contact, C:\\Users\Default\Contacts\Administrator.contact.avdn, C:\\Users\kEecfMwgj\Contacts\Administrator.contact	Modified File	72.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
257d60bf2fde40d0282bb05aeb69a0c350a82a03a96156b7d76c23441d2140d9	C:\\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url, C:\\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
5a64312c449747496728127ca6ca53bbea2a7c883020a46db87aaf7b53d5c3f1	C:\\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url, C:\\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
e04f6b8910d36f6096d6afa4f57bd3d347a7810caa4ffe6773e20c5a047269c0	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url, C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
192956dd8bc9fbd3819c47db66713e6fcc5fcaea3c0beedf8833067b6cb4780b	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url.avdn, C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
83567f9f7aba5b25d18788e4553a368f6620ec3e81982fb6e1acf07dd0fcdd72	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url.avdn, C:\\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
7faa30db6ec952b6f101b4843ab04c2a1c5ca0ebcf5d8846ffdc0b5c2401b91d	C:\\Users\Default\Favorites\MSN Websites\MSN Autos.url.avdn, C:\\Users\Default\Favorites\MSN Websites\MSN Autos.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
a026e99e2b81985eaf24a559f7b94021e4678a89d4b6d9cdb465bff598d98e45	C:\\Users\Default\Favorites\MSN Websites\MSN Entertainment.url.avdn, C:\\Users\Default\Favorites\MSN Websites\MSN Entertainment.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
921d4eb5eb76a3175ec4751ad417bbc50d828becfe375cd7b6a8c555267ea361	C:\\Users\Default\Favorites\MSN Websites\MSN Money.url, C:\\Users\Default\Favorites\MSN Websites\MSN Money.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f098125e203baa7ab39f64487d8f4bd1563d16244c66e5cfa9d391dad952f6a3	C:\\Users\Default\Favorites\MSN Websites\MSN Sports.url.avdn, C:\\Users\Default\Favorites\MSN Websites\MSN Sports.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d65df7c29218553d712f4da24708790c7885796d4c7425ed1268c14e0c89248c	C:\\Users\Default\Favorites\MSN Websites\MSN.url, C:\\Users\Default\Favorites\MSN Websites\MSN.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d9dfa3a6665b8bd39d0f0d3f80a3afc907d63e7d49c798b8e1504b225badd0f0	C:\\Users\Default\Favorites\MSN Websites\MSNBC News.url, C:\\Users\Default\Favorites\MSN Websites\MSNBC News.url.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
ea49d66b62cfe879946ba63bfced7501c660c2ec03da7a3051765367fcba5546	C:\\Users\Default\NTUSER.DAT.LOG.avdn, C:\\Users\Default\NTUSER.DAT.LOG	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d3be08dd25b5915e412c1132de55a2f330a358afb446cb926627b9b9b4788982	C:\\Users\Default\NTUSER.DAT.LOG1, C:\\Users\Default\NTUSER.DAT.LOG1.avdn	Modified File	192.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
57c69af0f317ccc0aa33cd947c31f9b02c8b0f833add27f9e5cc477771033302	C:\\Users\Default\NTUSER.DAT.LOG2, C:\\Users\Default\NTUSER.DAT.LOG2.avdn	Modified File	536 bytes	application/octet-stream	Access, Write, Delete, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
666045045b6042fcc9f374704a9279437745 77f52387b0183d618d348768f5a1	C:\ \Users\Default\Searches\Everywhere.search-ms, C:\ \Users\Default\Searches\Everywhere.search-ms.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
0721be5c78a690aad8495b4ca997cba2f3b6626f6d389a69dd59dfe1993486ef	C:\\Users\Default\Searches\Indexed Locations.search-ms, C:\ \Users\Default\Searches\Indexed Locations.search-ms.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
13e398b5049ecb6db494eb9231bfc0de8e804e74b82a51837abffbf43a8f25a3	C:\\Users\kEecfMwgj\Desktop\-Czpv.mp3, C:\ \Users\kEecfMwgj\Desktop\-Czpv.mp3.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
2f7215137d9585f448e8e51e6424ad1feb93b870a9683450fce796aa906da4f6	C:\\Users\kEecfMwgj\Desktop\-ozBRIuaHqu9LIfa7.flv, C:\ \Users\kEecfMwgj\Desktop\-ozBRIuaHqu9LIfa7.flv.avdn	Modified File	40.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
99c21e95839b9755fa2c23442f00d989812d6d71384f9e4ddba6d24019838d43	C:\ \Users\kEecfMwgj\Desktop\05Gh.mkv.avdn, C:\ \Users\kEecfMwgj\Desktop\05Gh.mkv	Modified File	48.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
7a08f1c46d158cf559e79b4d5834328c84ff3c1ba831cf8bd87040ec82b75c95	C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps.avdn, C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps	Modified File	72.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
155c3781ec3c88ec5be0243ed682b7ba578f05df47c7e869ecfa30281af9d9e4	C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf, C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c8adffad1f7f529380208fa82c75535ead186b0e51c15f6dace5562452c21460	C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe 59.mp3, C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe 59.mp3.avdn	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
47bdaf781b239e7ada8caa09ac1144e581c94eb1f47dd03eacc4a2f15c19942c	C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7l.wav, C:\ \Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7l.wav.avdn	Modified File	88.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2	C: \Users\kEecfMwgj\Desktop\Avaddon_09_06_2020_1054KB.exe, C: \Users\kEecfMwgj\AppData\Roaming\Avaddon_09_06_2020_1054KB.exe	Sample File	1053.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	MALICIOUS
d04199b8d17f90a3663a721add9b20f4d1f07d8f4714e45644cf3c38ce810fc4	C:\\Users\Default\Favorites\Links\Web Slice Gallery.url.avdn, C:\ \Users\Default\Favorites\Links\Web Slice Gallery.url	Modified File	8.52 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	c: \users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	50 bytes	application/octet-stream	-	CLEAN
e6327db35ddc7e174a160187944432f8ea2da6283c4bbeb96e2e50491b694412	C:\\Users\Default\Searches\041656-readme.html, C:\ \Users\Default\Favorites\Links\041656-readme.html, C:\ \Users\Default\Favorites\M... ... \3NR2RNc6BbR\041656-readme.html, C:\\Users\Default\041656-readme.html, C:\ \Users\Default\Favorites\MSN Websites\041656-readme.html	Dropped File	49.89 KB	text/html	Access, Write, Create	CLEAN
6a4a2c79766c3189f448cf9e5466cf16bcad560680e5e5b2dc5fae580fca6da4	c: \users\keecfmwgj\appdata\roaming\microsoft\windows\cookies\keecfmwgj@myip[1].txt	Dropped File	208 bytes	text/plain	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\Avaddon_09_06_2020_1054KB.exe	Sample File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Avaddon_09_06_2020_1054KB.exe	Sample File	Access, Write, Create	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN
C:\Users\Default\Contacts\Administrator.contact	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Contacts\Administrator.contact.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Contacts\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Links\Web Slice Gallery.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Links\Web Slice Gallery.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Links\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Autos.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Autos.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Entertainment.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Entertainment.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Money.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Money.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Sports.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN Sports.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSN.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSNBC News.url	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Favorites\MSN Websites\MSNBC News.url.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\NTUSER.DAT.LOG	Modified File	Read, Access, Write, Delete	CLEAN

File Name	Category	Operations	Verdict
C:\Users\Default\NTUSER.DAT.LOG.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\NTUSER.DAT.LOG1	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\NTUSER.DAT.LOG1.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\NTUSER.DAT.LOG2	Modified File	Access, Write, Delete	CLEAN
C:\Users\Default\NTUSER.DAT.LOG2.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Searches\Everywhere.search-ms	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Searches\Everywhere.search-ms.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\Default\Searches\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\Default\Searches\Indexed Locations.search-ms	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\Default\Searches\Indexed Locations.search-ms.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Contacts\Administrator.contact	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Contacts\Administrator.contact.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Contacts\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\-Czpv.mp3	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\-Czpv.mp3.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\-ozBRIuaHqu9LIfa7.flv	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\-ozBRIuaHqu9LIfa7.flv.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\05Gh.mkv	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\05Gh.mkv.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\aFqKTEVkXz4.pps.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\041656-readme.html	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\JGMjgzsvl.swf.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe59.mp3	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\MfvhZsjFMLaQe59.mp3.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7l.wav	Modified File	Read, Access, Write, Delete	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\N5gxiC7mfninX7l.wav.avdn	Modified File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\Desktop\3NR2RNc6BbR\RFJTv9x-gQ067-kfdq.ppt	Accessed File	Read, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.myip.com	-	104.21.23.5	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://www.torproject.org	-	-	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.myip.com	104.21.23.5	-	HTTPS	CLEAN
www.torproject.org	-	-	HTTPS	CLEAN
q9iatrkprh	192.168.0.129	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
104.21.23.5	api.myip.com	-	TCP, DNS, HTTPS	CLEAN
172.67.208.45	api.myip.com	United States	DNS	CLEAN
192.168.0.129	q9iatrkprh	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{2A0E9C7B-6BE8-4306-9F73-1057003F605B}	access	avaddon_09_06_2020_1054kb.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, write	avaddon_09_06_2020_1054kb.exe	MALICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, write	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access, create	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\update	access, write	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	access, create	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\update	access, write	avaddon_09_06_2020_1054kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections	access, write	avaddon_09_06_2020_1054kb.exe	CLEAN

Process

Process Name	Commandline	Verdict
avaddon_09_06_2020_1054kb.exe	"C:\Users\kEecfMwgj\Desktop\Avaddon_09_06_2020_1054KB.exe"	MALICIOUS
wmic.exe	wmic.exe SHADOWCOPY /nointeractive	CLEAN

Process Name	Commandline	Verdict
vssadmin.exe	vssadmin.exe Delete Shadows /All /Quiet	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN

YARA / AV

YARA (24)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\Default\Contacts\Administrator .contact	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\Microsoft Websites\IE Add-on site.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\Microsoft Websites\IE site on Microsoft.com.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Home.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft At Work.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\Microsoft Websites\Microsoft Store.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSN Autos.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSN Entertainment.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSN Money.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSN Sports.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSN.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Favorites\MSN Websites\MSNBC News.url	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\NTUSER.DAT.LOG	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\Default\NTUSER.DAT.LOG1	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\Default\NTUSER.DAT.LOG2	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\Default\Searches\Everywhere. search-ms	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\Default\Searches\Indexed Locations.search-ms	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\kEecfMwgj\Desktop\-Czpv.mp3	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\\Users\kEecfMwgj\Desktop\-ozBRIuaHqu9Lfa7.flv	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\kEecfMwgj\Desktop\05Gh.mkv	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\kEecfMwgj\Desktop\3NR2RN c6BbR\aFqKTEVkXz4.pps	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\kEecfMwgj\Desktop\3NR2RN c6BbR\JGMjgzsvl.swf	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\kEecfMwgj\Desktop\3NR2RN c6BbR\MfvhZsjFMLaQe 59.mp3	Ransomware	5/5
Ransomware	SodinokibiEncryptedFile	File encrypted by Sodinokibi Ransomware	Dropped File	C:\ \Users\kEecfMwgj\Desktop\3NR2RN c6BbR\N5gxiC7mfninX7I.wav	Ransomware	5/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
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	Not installed

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