MALICIOUS

Classifications: Ransomware

Threat Names: Gen:Heur.Variadic.A.175.1

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**Rasomware2.0.exe**
ID	#317572
MD5	f1790d7b0520f6d44a031d8abf20dda2
SHA1	5095ad3932ab58ebcd38ebbd563cbac486a054ef
SHA256	0228c17c158f3cc383afa6b45dd749ad4d5ed22a3b13cc3f1ad5ad7a242d0a85
File Size	145.50 KB
Report Created	2021-03-27 03:36 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (6 rules, 6 matches)

Score	Category	Operation	Count	Classification
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) rasomware2.0.exe modifies the content of multiple user files.			
4/5	System Modification	Disables a crucial system tool	1	-
	• (Process #1) rasomware2.0.exe disables the Task Manager via registry.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Gen:Heur.Variadic.A.175.1".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) rasomware2.0.exe has a thread which sleeps more than 5 minutes.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) rasomware2.0.exe enables process privilege "SeDebugPrivilege".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) rasomware2.0.exe adds "empty" to Windows startup via registry.			

Remarks

ⓘ **Anti-Sleep Triggered (0x0200000E):** The overall sleep time of all monitored processes was truncated from "2 hours, 26 minutes, 9 seconds" to "1 minute, 1 second" to reveal dormant functionality.

Mitre ATT&CK Matrix

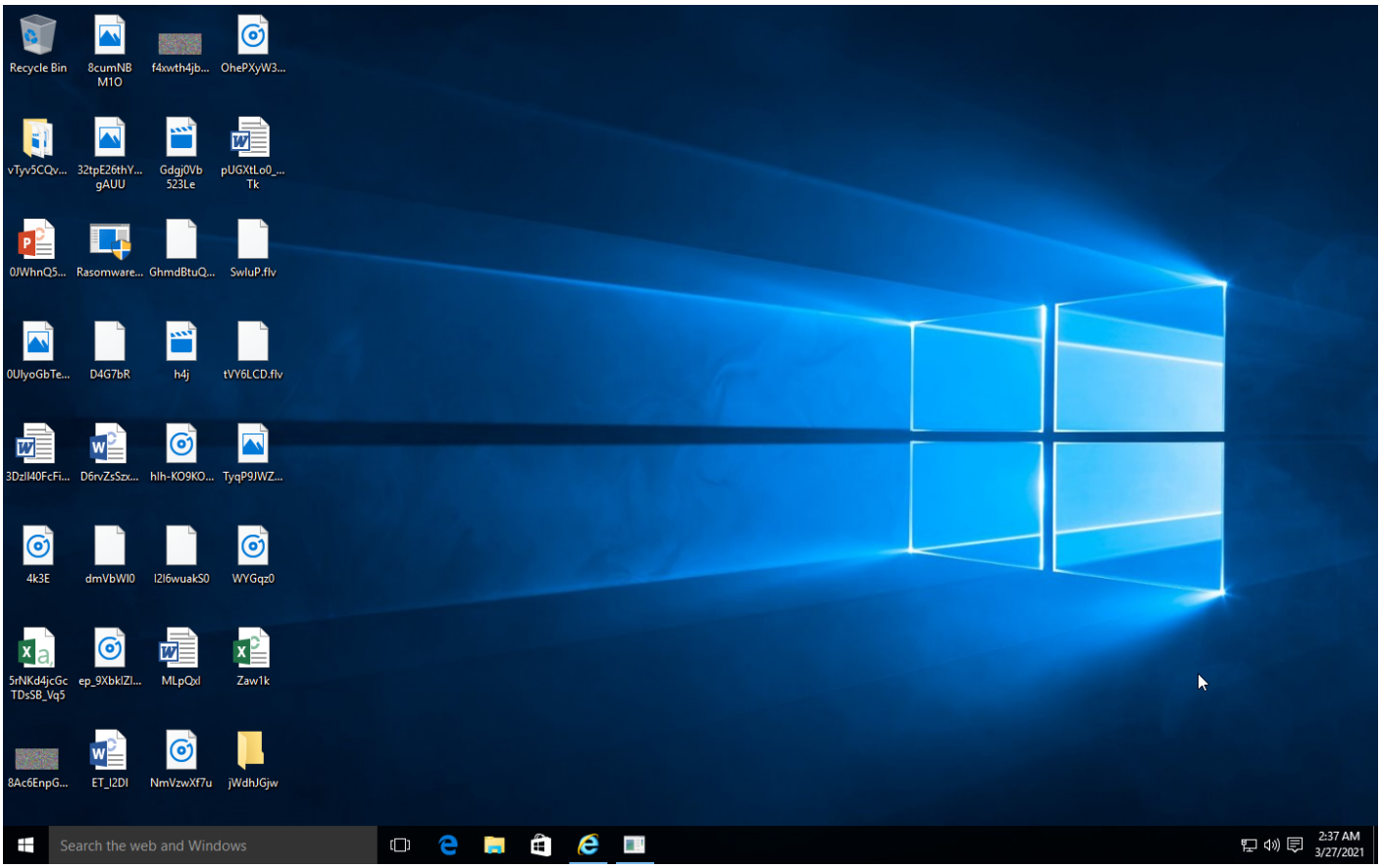
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	-	-	-	-	-	-	-	#T1490 Inhibit System Recovery
-	-	-	-	#T1112 Modify Registry	-	-	-	-	-	-	-
-	-	#T1060 Registry Run Keys / Startup Folder	-	-	-	-	-	-	-	-	-

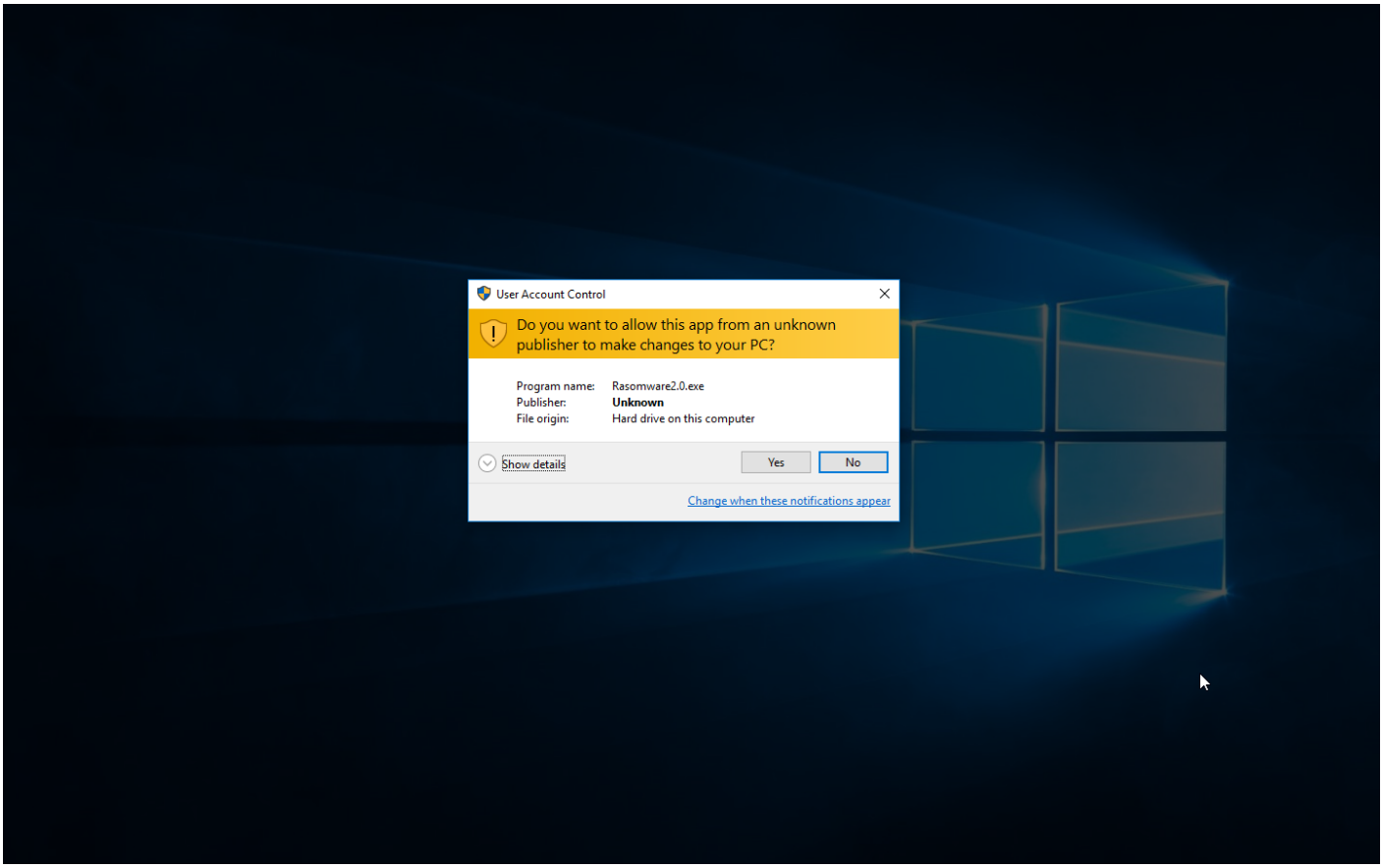
Sample Information

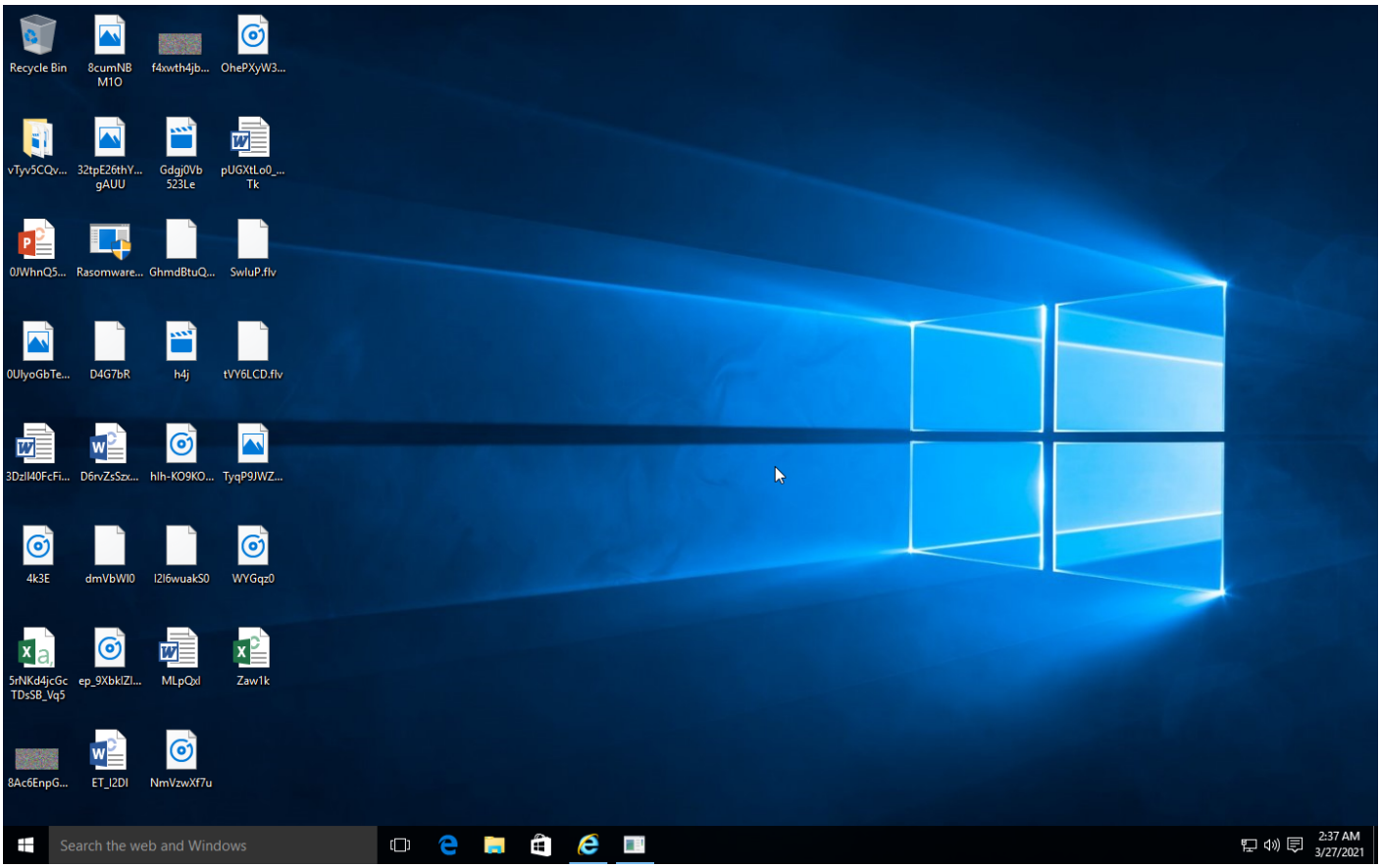
ID	967039
MD5	f1790d7b0520f6d44a031d8abf20dda2
SHA1	5095ad3932ab58ebcd38ebbd563cbac486a054ef
SHA256	0228c17c158f3cc383afa6b45dd749ad4d5ed22a3b13cc3f1ad5ad7a242d0a85
SSDeep	1536:VON/7xi3yBQjUho9JdZ582RsjCkOA36jCkOA3VdwVcl:VON/dWXEo9JdZ5r6jqAqjqAFdqY
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
Filename	Rasomware2.0.exe
File Size	145.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

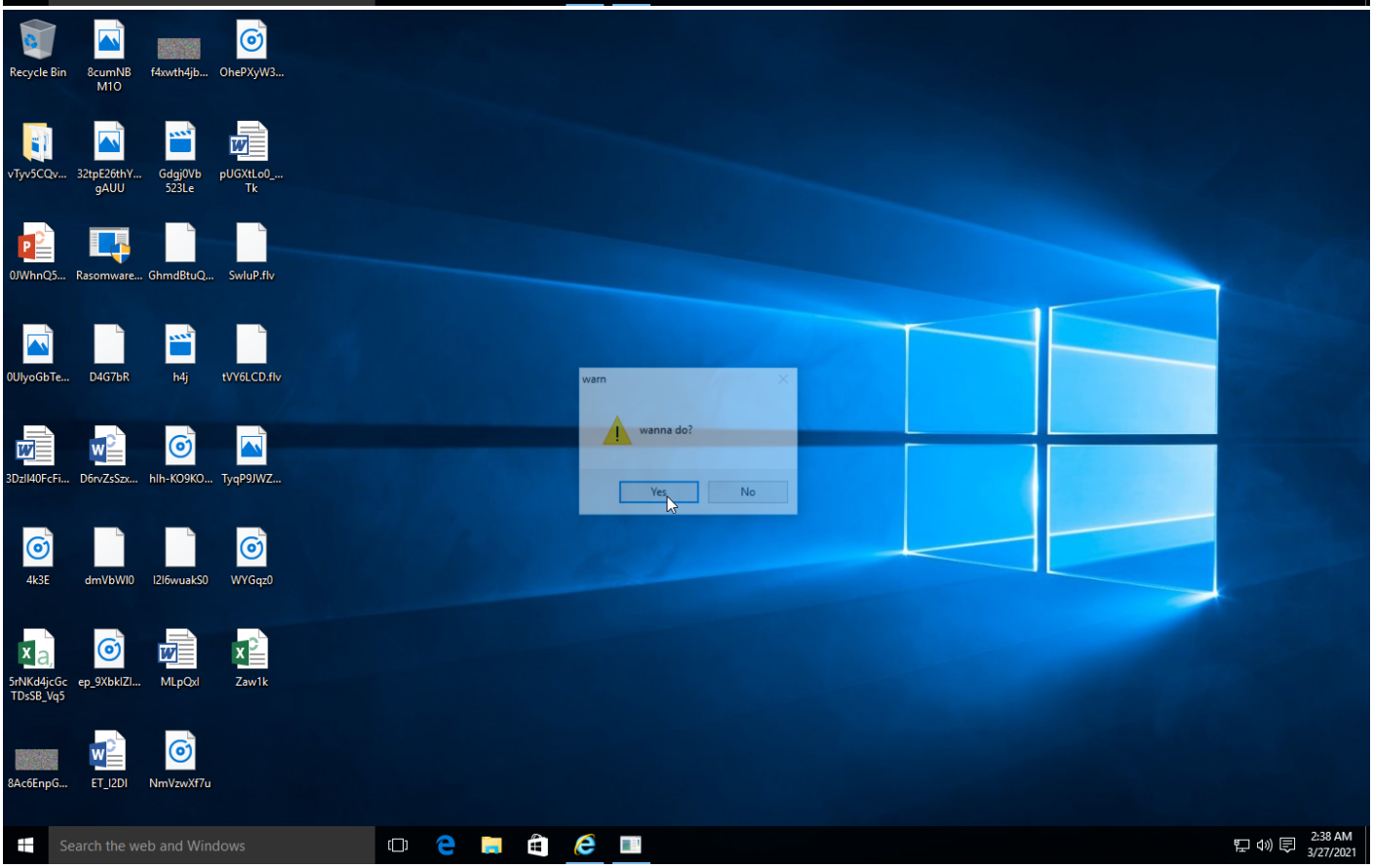
Analysis Information

Creation Time	2021-03-27 03:36 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successfull	False
Reputation Analysis 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	1
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
8cumNBM1O
f4xwth4jb...
OhePXyW3...
vTyv5CQv...
32tpE26thY...gAUU
Gdgj0Vb523Le
pUGXtLo0_...Tk
0JWhnQ5...
Rasomware...
GhmdBtuQ...
SwluP.flv
0UlyoGbTe...
D4G7bR
h4j
tVY6LCD.flv
3DzII40FcFi...
D6rvZsSzx...
hIh-KO9KO...
TyqP9JWZ...
4k3E
dmVbWI0
I2I6wuakS0
WYGqz0
5rNKd4jcGcTDsSB_Vq5
ep_9XbkIZI...
MLpQxl
Zaw1k
8Ac6EnpG...
ET_I2DI
NmVzwXf7u
jWdhJGjw
Search the web and Windows
2:37 AM
3/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: Rasomware2.0.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots trunkated.

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 recivied

DNS Requests

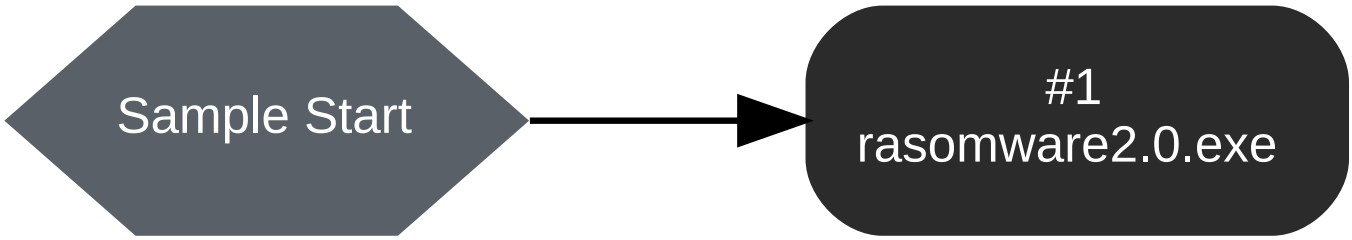
-

HTTP Requests

-

BEHAVIOR

Process Graph



Process #1: rasomware2.0.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\rasomware2.0.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Rasomware2.0.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 83335, Reason: Analysis Target
Unmonitor End Time	End Time: 323403, Reason: Terminated by Timeout
Monitor Duration	240.07s
Return Code	Unknown
PID	2280
Parent PID	2104
Bitness	64 Bit

Dropped Files (23)

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\0JWhnQ5nqU1_.odp	45.16 KB	6011dd50879f8960aa03a7787058cecfdc41c46a08ba10db93c9a3563ae5b415	✕
C:\Users\RDhJ0CNFevzX\Desktop\0UlyoGbTex7BaU.jpg	85.17 KB	9dea74feddd11526cd6254158c64e0460db403a1afbe77837b2b5d37e17029de	✕
C:\Users\RDhJ0CNFevzX\Desktop\32tpE26thYS3sTN gAUU.png	40.69 KB	226157731ceef9f97718de83064b8989831d49d64a2a00cd3311b547978653fe	✕
C:\Users\RDhJ0CNFevzX\Desktop\3DzIl40FcFiM-1-.rtf	66.31 KB	2190078429bb1ca5d7127721a571eb77a37b18acee8523ae606c03f33163f996	✕
C:\Users\RDhJ0CNFevzX\Desktop\4k3E.mp3	94.84 KB	1c9b0f7de5e531d288b2ffe9e33ab21c1e6a42c5234d8b57f39700977b4b9bba	✕
C:\Users\RDhJ0CNFevzX\Desktop\5rNKd4jcGcTDsSB_Vq5.csv	73.39 KB	87575bddc420f9f1f137741fcb04c532685d049e5393a3bb04ac4252dbe22687	✕
C:\Users\RDhJ0CNFevzX\Desktop\8Ac6EnpGGz93lKBUaK.bmp	59.53 KB	cf509f8583120bc98796bbcfaa84fda591da86e9251f08827ac11192a4607aa8	✕
C:\Users\RDhJ0CNFevzX\Desktop\8cumNBM1O.jpg	11.86 KB	43a9e71e746b919815ed789365029da8c72144637808bf78c786af59fd95dab4	✕
C:\Users\RDhJ0CNFevzX\Desktop\D4G7bR.swf	28.52 KB	592d3c27f9f108e3398501356a599c29e92b3bedd77f0b0d3cf7553e1cc04017	✕
C:\Users\RDhJ0CNFevzX\Desktop\D6rvZsSzxD1uC.odt	54.91 KB	eaa64591269acf63e0592a619db6c3f405d22378cafdc7ce374f930711ffcaeb	✕
C:\Users\RDhJ0CNFevzX\Desktop\dmVbWl0.swf	49.98 KB	1185aff14f36f8579709403b1b78b089ebaa71f574ef144b1b12f7c0d5fcccb4	✕
C:\Users\RDhJ0CNFevzX\Desktop\ep_9XbkIZIfoBe8FigT.m4a	74.08 KB	f5f20a32703d3921f0f6f845135397efde8f46402d69126c5791fb2fc9502a15	✕
C:\Users\RDhJ0CNFevzX\Desktop\ET_I2Dl.odt	7.53 KB	9081d2738e668c8bb025c70411535de7436721f2802f404cb8a333aea72f377d	✕
C:\Users\RDhJ0CNFevzX\Desktop\f4xwth4jbphujlS.bmp	58.77 KB	441a41127603e7941fad31cc20a08162b0e6eaf35b961c62d74bb719a6e4c6e3	✕
C:\Users\RDhJ0CNFevzX\Desktop\Gdgj0Vb523Le.mkv	46.66 KB	bbe9e6d6e6ba47d60108675c6c05d559365965bb4156062061116341c5726f90	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\GhmdBtuQWpt.swf	73.73 KB	76a5d348eb0918470e1fff42b356e9b2d9cf4d15393b1c1395547e990892f77c	✕
C:\Users\RDhJ0CNFevzX\Desktop\h4j.avi	44.33 KB	7c4def8c39a5588e7e538b24093efb620f4aab7861241a3307bd563c061d01b6	✕
C:\Users\RDhJ0CNFevzX\Desktop\hIh-KO9KOga7x29pb.wav	40.75 KB	8ae5f70ebd699614077331809ead94090de75fb9b5031a5e3d99d4dff7a157d9	✕
C:\Users\RDhJ0CNFevzX\Desktop\I2I6wuakS0.swf	65.52 KB	b8b207ea9944e070fa423a4a046ce402532ee448041aeda4a1894b7ec20fa255	✕
C:\Users\RDhJ0CNFevzX\Desktop\MLpQxI.rtf	41.11 KB	54ee4edbf9235b1eb3ca623917f2c5b7a90ac93fa942bc7579175f8bd00eb843	✕
C:\Users\RDhJ0CNFevzX\Desktop\NmVzwXf7u.mp3	65.67 KB	ad37edcab07df09b92802b04f221b9778ae9ecb32328226df63b3ebe7aedc0f9	✕
C:\Users\RDhJ0CNFevzX\Desktop\OhePXyW3h-f1uvKAlZ.wav	5.50 KB	f308ef04bbe3fe3c33f0d1075176543c98365167bc3bb685a6b5a8655bf13d74	✕
C:\Users\RDhJ0CNFevzX\Desktop\pUGXtLo0_-py Tk.rtf	23.06 KB	807eaa06e8f83079b795c234b9a10fb1f40e6659878f150616779299502f7a34	✕

Host Behavior

Type	Count
Module	5733
System	16573
Window	5000
Registry	23
File	495
Keyboard	170
User	1
Environment	4

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
0228c17c158f3cc383afa6b45dd749ad4d5ed22a3b13cc3f1ad5ad7a242d0a85	C:\Users\RDhJ0CNFevzX\Desktop\Rasomware2.0.exe	Sample File	145.50 KB	application/vnd.microsoft.portable-executable	Create, Read, Access	MALICIOUS
129d212cdef43e689852cb493e2c633dd4a5ce38e7fc4d3024ec29f33a3b0c0d	C:\Users\RDhJ0CNFevzX\Desktop\0JWhnQ5nqU1_.odp	Modified File	45.14 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
5210a9bbcc9641798838a919b5ce30e86ddf566619a00259a0183c37d3867440	C:\Users\RDhJ0CNFevzX\Desktop\0UlyoGbTex7BaU.jpg	Modified File	85.16 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
0b97af4bc79a44afe8e1be8efa7814c4fbf245395cb95c940d42dcfffaf478f9	C:\Users\RDhJ0CNFevzX\Desktop\32tpE26thYS3sTN gAUU.png	Modified File	40.67 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
e22f364eaaf4e6e02d20d50858698911127fda2c22e75e50f58f141ecae8d0a6	C:\Users\RDhJ0CNFevzX\Desktop\3DzII40FcFiM-1-.rtf	Modified File	66.30 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
de44816725e866c2cbb51ff19d17cb69cb2453f602a2371aebd075867b3211f3	C:\Users\RDhJ0CNFevzX\Desktop\4k3E.mp3	Modified File	94.83 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
b56645ea56a09fedd378612851d623fedbc85cc8b378c53fee5d46bc0c0b355b	C:\Users\RDhJ0CNFevzX\Desktop\5rNKd4jcGcTDsSB_Vq5.csv	Modified File	73.38 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
d8a4cbb5b2f96d87762aa917288a5e1fb519b3805c99a4ce0be5093f3ff38323	C:\Users\RDhJ0CNFevzX\Desktop\8Ac6EnpGGz93lKBUaK.bmp	Modified File	59.52 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
a6ab49c7cda2385a535fad8bf0dc4412b38e0196839fd59a3f9482fa00f3ef7c	C:\Users\RDhJ0CNFevzX\Desktop\8cumNBM1O.jpg	Modified File	11.84 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
6d221ae9aaed7b6bd4bd2648ab0a21460c8d0635c68cb067a1c4c1b449d15171	C:\Users\RDhJ0CNFevzX\Desktop\D4G7bR.swf	Modified File	28.50 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
be0639880570c8496a96bbc15bc95700f098a664402a972f345cc712833f8af4	C:\Users\RDhJ0CNFevzX\Desktop\D6rvZsSzxD1uC.odt	Modified File	54.89 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
7500c7adcf9b1e26ceca833686b3bc6178cef99913c61b3db3a7d615a75988ec	C:\Users\RDhJ0CNFevzX\Desktop\dmVbWl0.swf	Modified File	49.97 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
060394673b4f699ad3369a6e2085e8e661cd9e845ff3f1b9458d5386807b7a8a	C:\Users\RDhJ0CNFevzX\Desktop\ep_9XbkIZIfoBe8FigT.m4a	Modified File	74.06 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
87adbef0ed61e6492a6630e3089f8ee22840d1a05129866f6d33ce832f943fc4	C:\Users\RDhJ0CNFevzX\Desktop\ET_I2Dl.odt	Modified File	7.52 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
af21dd23955d8253548d43474f315872afc98d535c4c5388caecd87ae7484898	C:\Users\RDhJ0CNFevzX\Desktop\f4xwth4jbphujlS.bmp	Modified File	58.75 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
6bde71479e98cd3bc8351256c7fe5cf9eb315d6bcbbbd56ed9384722967825ef	C:\Users\RDhJ0CNFevzX\Desktop\Gdgj0Vb523Le.mkv	Modified File	46.64 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
ec82b9177db61fe15ba949b57cf7f00ef7cad203ace5ebd3c217e0e20cc6c18c	C:\Users\RDhJ0CNFevzX\Desktop\GhmdBtuQWpt.swf	Modified File	73.72 KB	application/octet-stream	Create, Write, Read, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
e160d8592a0d5593ce2edac28e16240154e8400ea393bf23807656bb45a997ae	C:\Users\RDhJ0CNFevzX\Desktop\h4j.avi	Modified File	44.31 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
ed756c000c153fea66b4cda3e30aaf7c1b4051bcd0421155bdf0079f4291711c	C:\Users\RDhJ0CNFevzX\Desktop\hIh-KO9KOga7x29pb.wav	Modified File	40.73 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
3626a587eb444072d53df74de39a9c995b8d961c2ecb67eb1540eecf7a6c2451	C:\Users\RDhJ0CNFevzX\Desktop\l2I6wuakS0.swf	Modified File	65.50 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
594c0955db1438a09ad2139f56095ad3bf8a1624e816c973fda5b0cb40a6274b	C:\Users\RDhJ0CNFevzX\Desktop\MLpQxI.rtf	Modified File	41.09 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
beded60e2e043a65c4194096e0bb45706fd604bd5529486c07c342288c947375	C:\Users\RDhJ0CNFevzX\Desktop\NmVzwXf7u.mp3	Modified File	65.66 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
0ec1bef9d25027a6a7884437dbdc08a2d84b87e14bfbf9a2c10f0dcd4f2e42b4	C:\Users\RDhJ0CNFevzX\Desktop\OhePXyW3h-f1uvKAlZ.wav	Modified File	5.48 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
1dbf103e97384a11c98829ec0e4d57d83d8d905eebbe7efb148dbd4d80da492e	C:\Users\RDhJ0CNFevzX\Desktop\pUGXtLo0_-pyTk.rtf	Modified File	23.05 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
6011dd50879f8960aa03a7787058cecfdc41c46a08ba10db93c9a3563ae5b415	C:\Users\RDhJ0CNFevzX\Desktop\0JWhnQ5nqU1_.odp	Dropped File	45.16 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
9dea74feddd11526cd6254158c64e0460db403a1afbe77837b2b5d37e17029de	C:\Users\RDhJ0CNFevzX\Desktop\0UlyoGbTex7BaU.jpg	Dropped File	85.17 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
226157731ceef9f97718de83064b8989831d49d64a2a00cd3311b547978653fe	C:\Users\RDhJ0CNFevzX\Desktop\32tpE26thYS3sTN gAUU.png	Dropped File	40.69 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
2190078429bb1ca5d71227721a571eb77a37b18acee8523ae606c03f33163f996	C:\Users\RDhJ0CNFevzX\Desktop\3DzIl40FcFiM-1-.rtf	Dropped File	66.31 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
1c9b0f7de5e531d288b2ffe9e33ab21c1e6a42c5234d8b57f39700977b4b9bba	C:\Users\RDhJ0CNFevzX\Desktop\4k3E.mp3	Dropped File	94.84 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
87575bddc420f9f1f137741fcb04c532685d049e5393a3bb04ac4252dbe22687	C:\Users\RDhJ0CNFevzX\Desktop\5rNKd4jcGcTDsSB_Vq5.csv	Dropped File	73.39 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
cf509f8583120bc98796bbcfaa84fda591da86e9251f08827ac11192a4607aa8	C:\Users\RDhJ0CNFevzX\Desktop\8Ac6EnpGGz93lKBUaK.bmp	Dropped File	59.53 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
43a9e71e746b919815ed789365029da8c72144637808bf78c786af59fd95dab4	C:\Users\RDhJ0CNFevzX\Desktop\8cumNBM1O.jpg	Dropped File	11.86 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
592d3c27f9f108e3398501356a599c29e92b3bedd77f0b0d3cf7553e1cc04017	C:\Users\RDhJ0CNFevzX\Desktop\D4G7bR.swf	Dropped File	28.52 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
eaa64591269acf63e0592a619db6c3f405d22378cafdc7ce374f930711ffcaeb	C:\Users\RDhJ0CNFevzX\Desktop\D6rvZsSzxD1uC.odt	Dropped File	54.91 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
1185aff14f36f8579709403b1b78b089ebaa71f574ef144b1b12f7c0d5fcccb4	C:\Users\RDhJ0CNFevzX\Desktop\dmVbWl0.swf	Dropped File	49.98 KB	application/octet-stream	Create, Write, Read, Access	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f5f20a32703d3921f0f6f845135397efde8f46402d69126c5791fb2fc9502a15	C:\Users\RDhJ0CNFevzX\Desktop\ep_9XbkIZIfoBe8FigT.m4a	Dropped File	74.08 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
9081d2738e668c8bb025c70411535de7436721f2802f404cb8a333aea72f377d	C:\Users\RDhJ0CNFevzX\Desktop\ET_I2Dl.odt	Dropped File	7.53 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
441a41127603e7941fad31cc20a08162b0e6eaf35b961c62d74bb719a6e4c6e3	C:\Users\RDhJ0CNFevzX\Desktop\f4xwth4jbphujlS.bmp	Dropped File	58.77 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
bbe9e6d6e6ba47d60108675c6c05d559365965bb4156062061116341c5726f90	C:\Users\RDhJ0CNFevzX\Desktop\Gdgj0Vb523Le.mkv	Dropped File	46.66 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
76a5d348eb0918470e1ff42b356e9b2d9cf4d15393b1c1395547e990892f77c	C:\Users\RDhJ0CNFevzX\Desktop\GhmdBtuQWpt.swf	Dropped File	73.73 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
7c4def8c39a5588e7e538b24093efb620f4aab7861241a3307bd563c061d01b6	C:\Users\RDhJ0CNFevzX\Desktop\h4j.avi	Dropped File	44.33 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
8ae5f70ebd699614077331809ead94090de75fb9b5031a5e3d99d4dff7a157d9	C:\Users\RDhJ0CNFevzX\Desktop\hIh-KO9KOga7x29pb.wav	Dropped File	40.75 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
b8b207ea9944e070fa423a4a046ce402532ee448041aeda4a1894b7ec20fa255	C:\Users\RDhJ0CNFevzX\Desktop\I2I6wuakS0.swf	Dropped File	65.52 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
54ee4edbf9235b1eb3ca623917f2c5b7a90ac93fa942bc7579175f8bd00eb843	C:\Users\RDhJ0CNFevzX\Desktop\MLpQxI.rtf	Dropped File	41.11 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
ad37edcab07df09b92802b04f221b9778ae9ecb32328226df63b3ebe7aedc0f9	C:\Users\RDhJ0CNFevzX\Desktop\NmVzwXf7u.mp3	Dropped File	65.67 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
f308ef04bbe3fe3c33f0d1075176543c98365167bc3bb685a6b5a8655bf13d74	C:\Users\RDhJ0CNFevzX\Desktop\OhePXyW3h-f1uvKAlZ.wav	Dropped File	5.50 KB	application/octet-stream	Create, Write, Read, Access	CLEAN
807eaa06e8f83079b795c234b9a10fb1f40e6659878f150616779299502f7a34	C:\Users\RDhJ0CNFevzX\Desktop\pUGXtLo0_-pyTk.rtf	Dropped File	23.06 KB	application/octet-stream	Create, Write, Read, Access	CLEAN

Filename

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Rasomware2.0.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\0JWhnQ5nqU1_.odp	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\0UlyoGbTex7BaU.jpg	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\32tpE26thYS3sTN gAUU.png	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\3DzIl40FcFiM-1-.rtf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\4k3E.mp3	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\5rNKd4jcGcTDsSB_Vq5.csv	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8Ac6EnpGGz93lKBUaK.bmp	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8cumNBM1O.jpg	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\D4G7bR.swf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\D6rvZsSzxD1uC.odt	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\dmVbWl0.swf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ep_9XbkIZIfoBe8FigT.m4a	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ET_I2Dl.odt	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\f4xwth4jbphujlS.bmp	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Gdgj0Vb523Le.mkv	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\GhmdBtuQWpt.swf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\h4j.avi	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\hIh-KO9KOga7x29pb.wav	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\I2I6wuakS0.swf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\MLpQxI.rtf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\NmVzwXf7u.mp3	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\OhePXyW3h-f1uvKAlZ.wav	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\pUGXtLo0_-py Tk.rtf	Dropped File, Modified File	Create, Write, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Rasomware2.0.exe	Sample File	Create, Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SwluP.flv	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\tVY6LCD.flv	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\TyqP9JWZb53K.png	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WYGqz0.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Zaw1k.ods	Accessed File	Access	CLEAN

URL

-

Domain

-

IP

-

Email

-

Email Address

-

Mutex

-

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr	write, read, access	rasomware2.0.exe	MALICIOUS
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	rasomware2.0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	create, access	rasomware2.0.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop	access	rasomware2.0.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper	write, read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	write, read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	rasomware2.0.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	rasomware2.0.exe	CLEAN

Process

Process Name	Commandline	Verdict
rasomware2.0.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Rasomware2.0.exe"	MALICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Heur.Variadic.A.175.1	C:\Users\RDhJ0CNFevzX\Desktop\Rasomware 2.0.exe	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
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

Analyzer Information

Analyzer Version	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-03-27 00:41:44+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
Analysis Report Layout Version	10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed