Analysis Report

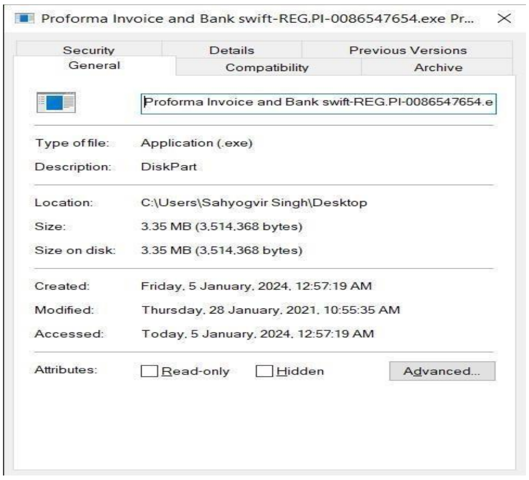
In this example, a suspicious file was analyzed. The sample was taken from any.run as a zip file ‘Request for Quotation (RFQ_196).zip’ and then I extracted the zip and the file I got was an executable file named as ‘Proforma Invoice and Bank swift-REG.PI-0086547654.exe’.

Basic Information

- Name: Proforma Invoice and Bank swift-REG.PI-0086547654
- Type: Executable file (.exe)
- SHA256 Hash: ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E0 80E41AA
- SHA1 Hash: 5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
- MD5 Hash: 84C82835A5D21BBCF75A61706D8AB549
- Size: 3.35 MB

Static Analysis

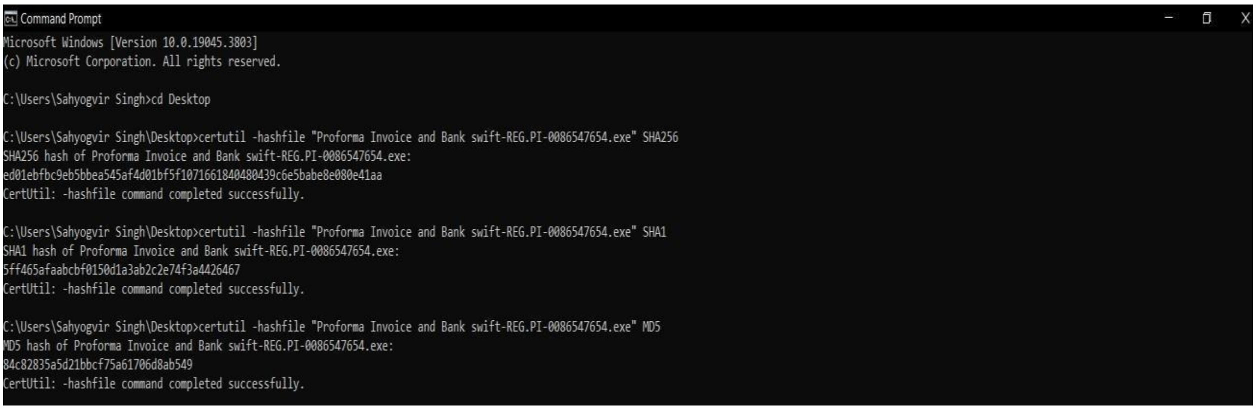
[1] Firstly, I checked the properties of the file and it was an executable file lastly modified on 28 Jan 2021 and it was disguised as Proforma Invoice and Bank swift-REG.PI-0086547654



Proforma Invoice and Bank swift-REG.PI-0086547654.e

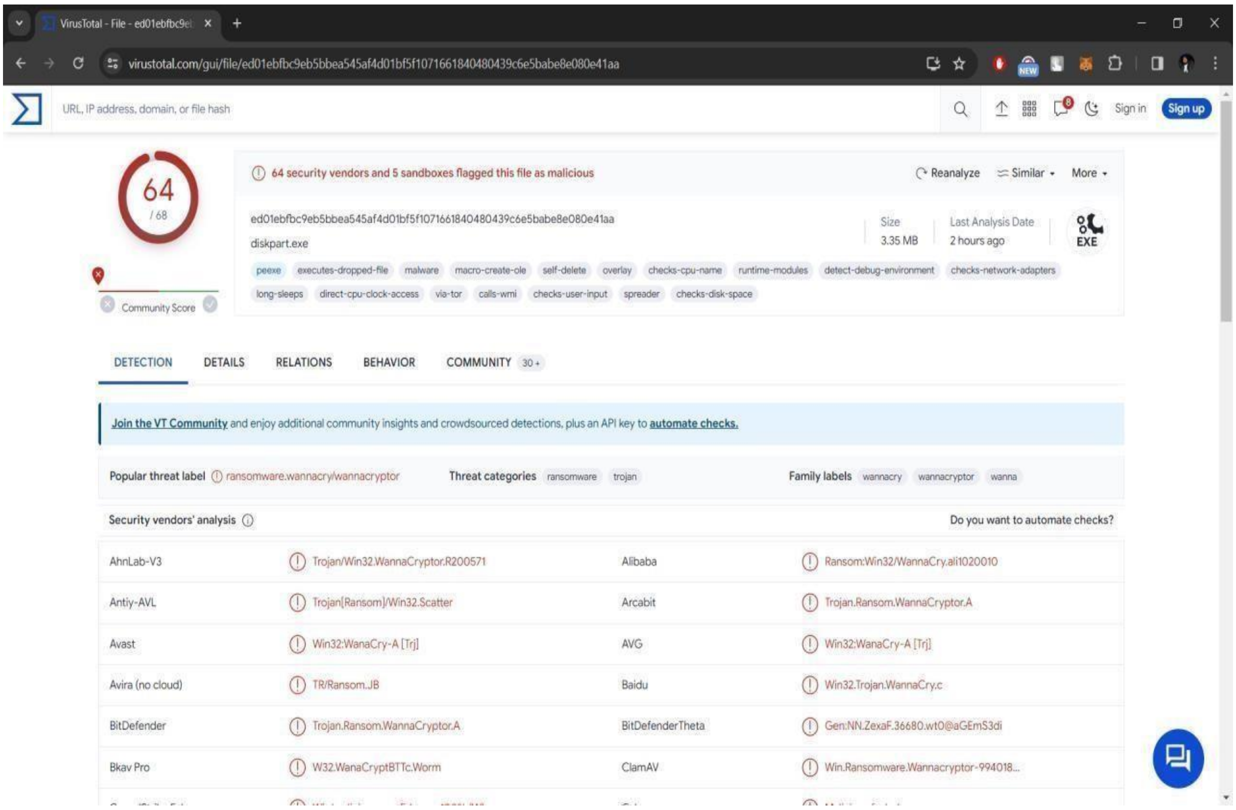
Type of file:	Application (.exe)
Description:	DiskPart
Location:	C:\Users\Sahyogvir Singh\Desktop
Size:	3.35 MB (3,514,368 bytes)
Size on disk:	3.35 MB (3,514,368 bytes)
Created:	Friday, 5 January, 2024, 12:57:19 AM
Modified:	Thursday, 28 January, 2021, 10:55:35 AM
Accessed:	Today, 5 January, 2024, 12:57:19 AM
Attributes:	□ Read-only □ Hidden

[2] Then I found SHA256, SHA1 and MD5 hashes of the file using ‘certutil hashfile’ command in command prompt.



```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sahyogvir Singh>cd Desktop

C:\Users\Sahyogvir Singh\Desktop>certutil -hashfile "Proforma Invoice and Bank swift-REG.PI-0086547654.exe" SHA256
SHA256 hash of Proforma Invoice and Bank swift-REG.PI-0086547654.exe:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
CertUtil: -hashfile command completed successfully.

C:\Users\Sahyogvir Singh\Desktop>certutil -hashfile "Proforma Invoice and Bank swift-REG.PI-0086547654.exe" SHA1
SHA1 hash of Proforma Invoice and Bank swift-REG.PI-0086547654.exe:
5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
CertUtil: -hashfile command completed successfully.

C:\Users\Sahyogvir Singh\Desktop>certutil -hashfile "Proforma Invoice and Bank swift-REG.PI-0086547654.exe" MD5
MD5 hash of Proforma Invoice and Bank swift-REG.PI-0086547654.exe:
84c82835a5d21bbcf75a61706d8ab549
CertUtil: -hashfile command completed successfully.
```

[3] On checking the hash of the file on VirusTotal the detection rate of the file came as 64/68 and it also flagged it as malicious. Another tool metadefender also marked the file as suspicious.



VirusTotal - File - ed01ebfbc9e
virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
URL, IP address, domain, or file hash
Sign in
Sign up
64
/ 68
Community Score
Reanalyze
Similar
More
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30 +

64 security vendors and 5 sandboxes flagged this file as malicious

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe

Size 3.35 MB | Last Analysis Date 2 hours ago | EXE

peexe · executes-dropped-file · malware · macro-create-ole · self-delete · overlay · checks-cpu-name · runtime-modules · detect-debug-environment · checks-network-adapters · long-sleeps · direct-cpu-clock-access · via-tor · calls-wmi · checks-user-input · spreader · checks-disk-space

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

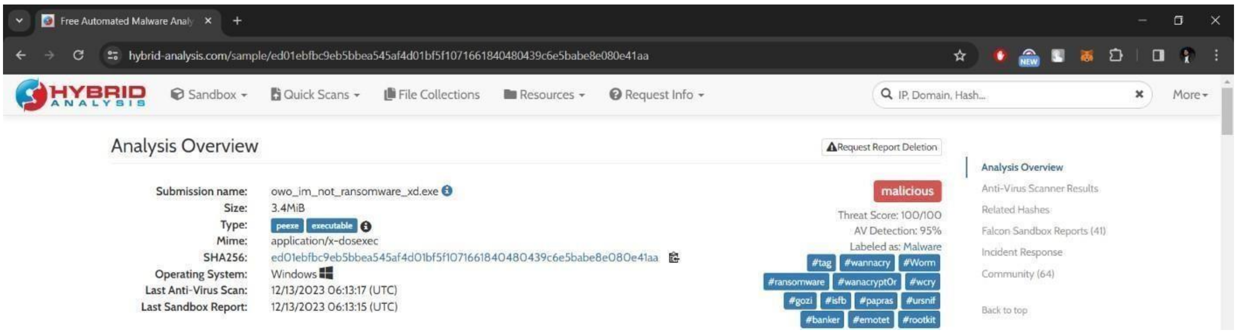
Popular threat label ransomware.wannacry/wannacryptor | Threat categories ransomware trojan | Family labels wannacry wannacryptor wanna

Security vendors' analysis | Do you want to automate checks?

AhnLab-V3	Trojan/Win32.WannaCryptor.R200571	Alibaba	Ransom:Win32/WannaCry.ali1020010
Antiy-AVL	Trojan[Ransom]/Win32.Scatter	Arcabit	Trojan.Ransom.WannaCryptor.A
Avast	Win32:WanaCry-A [Trj]	AVG	Win32:WanaCry-A [Trj]
Avira (no cloud)	TR/Ransom.JB	Baidu	Win32.Trojan.WannaCry.c
BitDefender	Trojan.Ransom.WannaCryptor.A	BitDefenderTheta	Gen:NN.ZexaF.36680.wt0@aGEmS3di
Bkav Pro	W32.WanaCryptBTTc.Worm	ClamAV	Win.Ransomware.Wannacryptor-994018...

Dynamic Analysis

[4] For further analysis the file was executed in some sandbox environments, starting with hybrid analysis which gave the file a threat score of 100/100 and marked it as malicious.

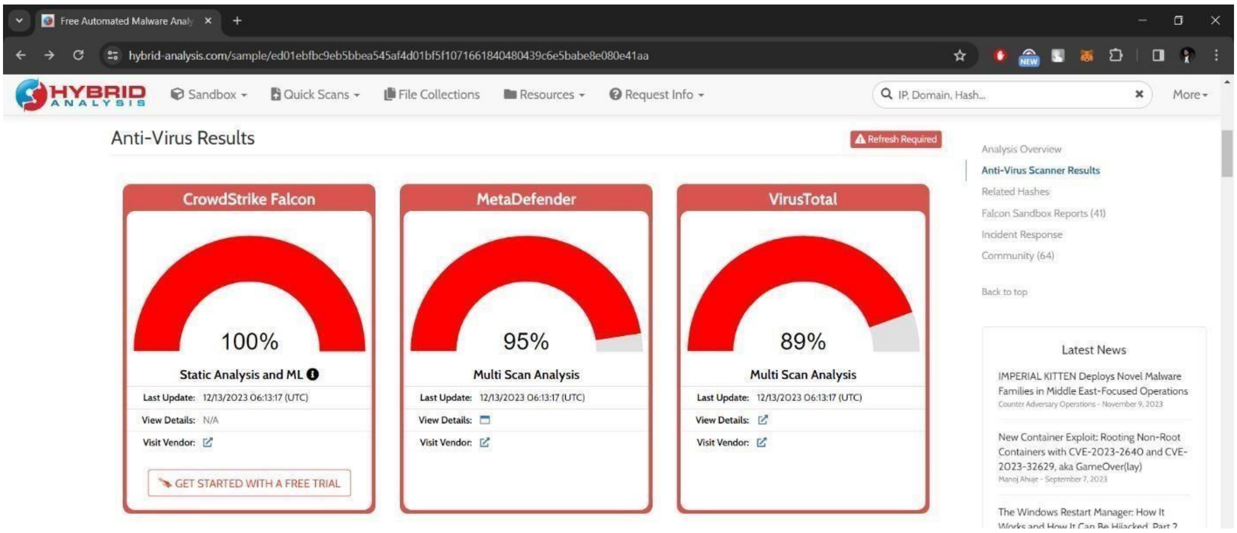


Analysis Overview

Submission name: owo_im_not_ransomware_xd.exe
Size: 3.4MiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Operating System: Windows
Last Anti-Virus Scan: 12/13/2023 06:13:17 (UTC)
Last Sandbox Report: 12/13/2023 06:13:15 (UTC)

malicious
Threat Score: 100/100
AV Detection: 95%
Labeled as: Malware
#tag #wannacry #Worm #ransomware #wanacryptOr #wcry #gozi #isfb #papras #ursnif #banker #emotet #rootkit

[5] It also scanned it using different anti viruses and all of them reported it as a malicious file.


Free Automated Malware Analy
hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
IP, Domain, Hash...
More
Refresh Required
Analysis Overview
Anti-Virus Scanner Results
Related Hashes
Falcon Sandbox Reports (41)
Incident Response
Community (64)
Back to top
GET STARTED WITH A FREE TRIAL

Anti-Virus Results

CrowdStrike Falcon
100%
Static Analysis and ML
Last Update: 12/13/2023 06:13:17 (UTC)
View Details: N/A
Visit Vendor:

MetaDefender
95%
Multi Scan Analysis
Last Update: 12/13/2023 06:13:17 (UTC)
View Details:
Visit Vendor:

VirusTotal
89%
Multi Scan Analysis
Last Update: 12/13/2023 06:13:17 (UTC)
View Details:
Visit Vendor:

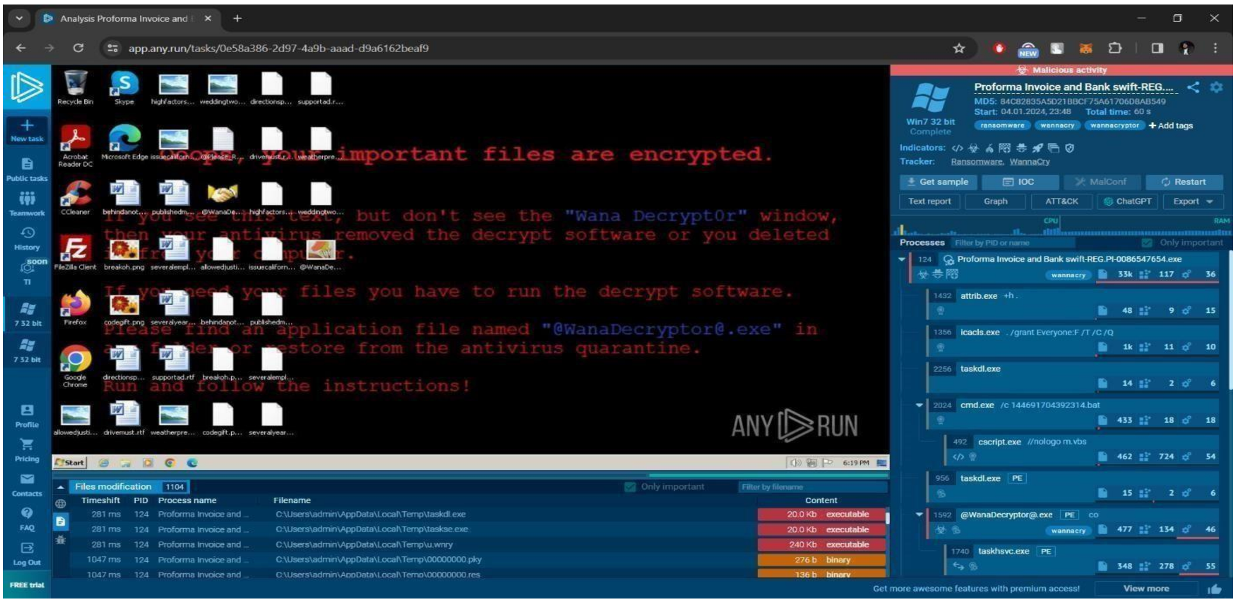
Latest News

IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
Counter Adversary Operations - November 9, 2023

New Container Exploit: Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver(lay)
Manoj Ahuje - September 7, 2023

The Windows Restart Manager: How It Works and How It Can Be Hijacked, Part 2

[6] Then I executed the file in sandbox environment 'any.run', where it was tagged as ransomware and wannacry with its hash values (MD5, SHA1 & SHA256) as the main IOCs, while other indicators include dropping executable file, starts cmd.exe for commands execution, reads the internet settings, create some files, modifies access control lists and also changing the wallpaper of the desktop.



app.any.run/tasks/0e58a386-2d97-4a9b-aaad-d9a6162beaf9

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Malicious activity

Proforma Invoice and Bank swift-REG....
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 04.01.2024, 23:48 Total time: 60 s
Win7 32 bit Complete
ransomware wannacry wannacryptor + Add tags
Tracker: Ransomware, WannaCry

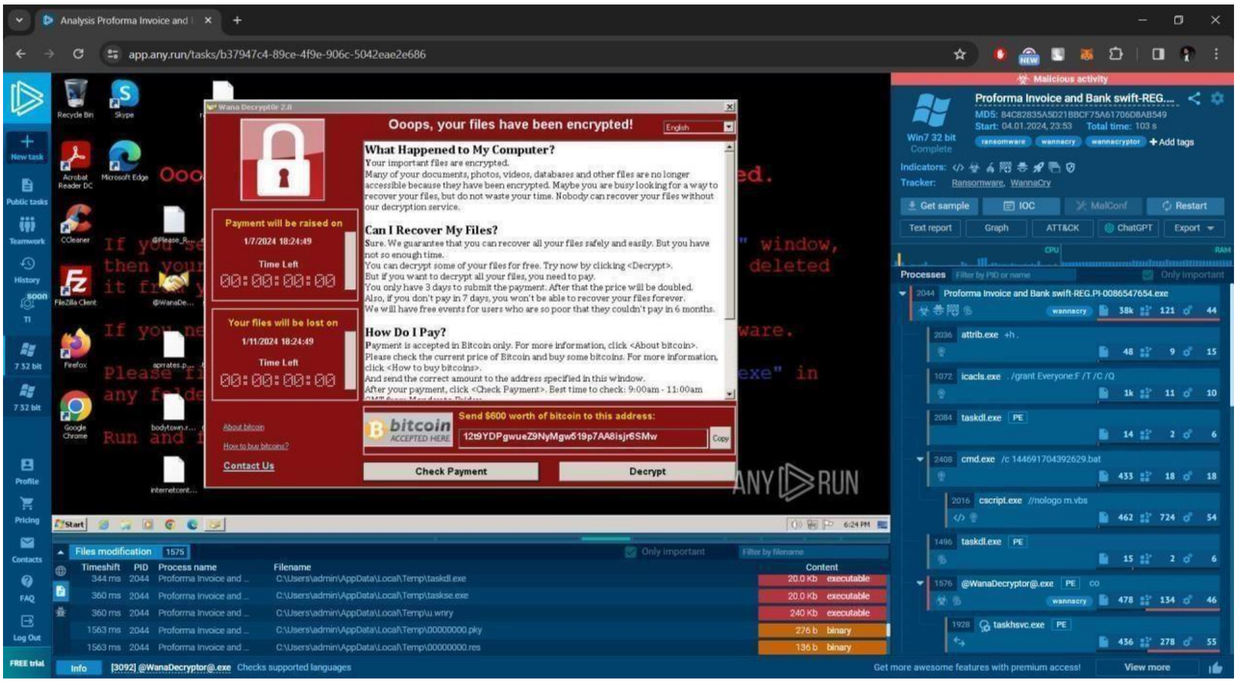
Processes

124 Proforma Invoice and Bank swift-REG.PI-0086547654.exe wannacry 33k 117 36
1432 attrib.exe +h . 48 9 15
1356 icacls.exe . /grant Everyone:F /T /C /Q 1k 11 10
2256 taskdl.exe 14 2 6
2024 cmd.exe /c 144691704392314.bat 433 18 18
492 cscript.exe //nologo m.vbs 462 724 54
956 taskdl.exe PE 15 2 6
1592 @WanaDecryptor@.exe PE co wannacry 477 134 46
1740 taskhsvc.exe PE 348 278 55

Files modification 1104

Timeshift	PID	Process name	Filename	Content
281 ms	124	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\taskdl.exe	20.0 Kb executable
281 ms	124	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\taskse.exe	20.0 Kb executable
281 ms	124	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\u.wnry	240 Kb executable
1047 ms	124	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\00000000.pky	276 b binary
1047 ms	124	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\00000000.res	136 b binary

[7] After execution a window popped up named ‘wana decryptor 2.0’ which asked for the payment in bitcoins worth $300 to recover the files or they would be lost and also had some links regarding ‘about bitcoin’, ‘how to buy bitcoin’ which redirected us to Wikipedia.



app.any.run/tasks/b37947c4-89ce-4f9e-906c-5042eae2e686

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
1/7/2024 18:24:49
Time Left
00:00:00:00

Your files will be lost on
1/11/2024 18:24:49
Time Left
00:00:00:00

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Malicious activity

Proforma Invoice and Bank swift-REG....
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 04.01.2024, 23:53 Total time: 103 s
Win7 32 bit Complete
ransomware wannacry wannacryptor + Add tags
Tracker: Ransomware, WannaCry

Processes

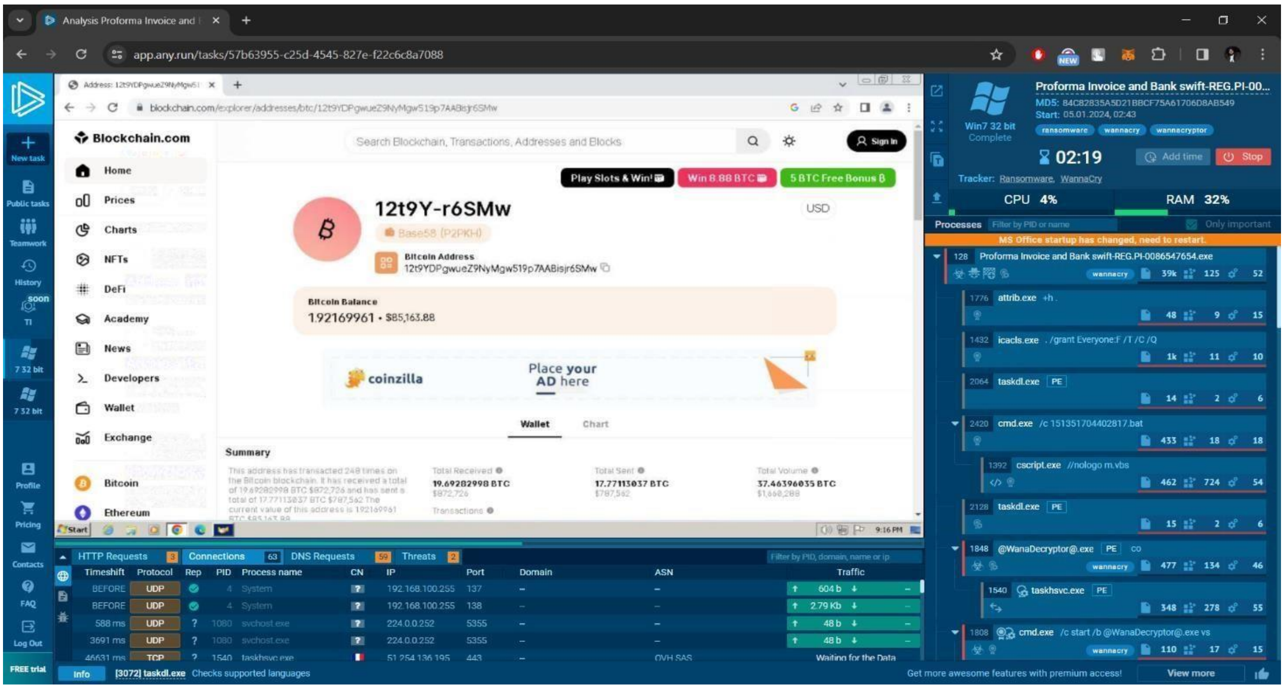
2044 Proforma Invoice and Bank swift-REG.PI-0086547654.exe wannacry 38k 121 44
2036 attrib.exe +h . 48 9 15
1072 icacls.exe . /grant Everyone:F /T /C /Q 1k 11 10
2084 taskdl.exe PE 14 2 6
2408 cmd.exe /c 144691704392629.bat 433 18 18
2016 cscript.exe //nologo m.vbs 462 724 54
1496 taskdl.exe PE 15 2 6
1576 @WanaDecryptor@.exe PE co wannacry 478 134 46
1928 taskhsvc.exe PE 436 278 55

Files modification 1575

Timeshift	PID	Process name	Filename	Content
344 ms	2044	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\taskdl.exe	20.0 Kb executable
360 ms	2044	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\taskse.exe	20.0 Kb executable
360 ms	2044	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\u.wnry	240 Kb executable
1563 ms	2044	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\00000000.pky	276 b binary
1563 ms	2044	Proforma Invoice and ...	C:\Users\admin\AppData\Local\Temp\00000000.res	136 b binary

Info [3092] @WanaDecryptor@.exe Checks supported languages

[8] It provided us with a wallet address to which we have to send bitcoins. On searching that address on ‘blockchain.com’ it showed us its details.



app.any.run/tasks/57b63955-c25d-4545-827e-f22c6c8a7088

blockchain.com/explorer/addresses/btc/12t9YDPgwueZ9NyMgw519p7AABisjr6SMw

12t9Y-r6SMw

Base58 (P2PKH)

Bitcoin Address
12t9YDPgwueZ9NyMgw519p7AABisjr6SMw

Bitcoin Balance
1.92169961 • $85,163.88

Summary

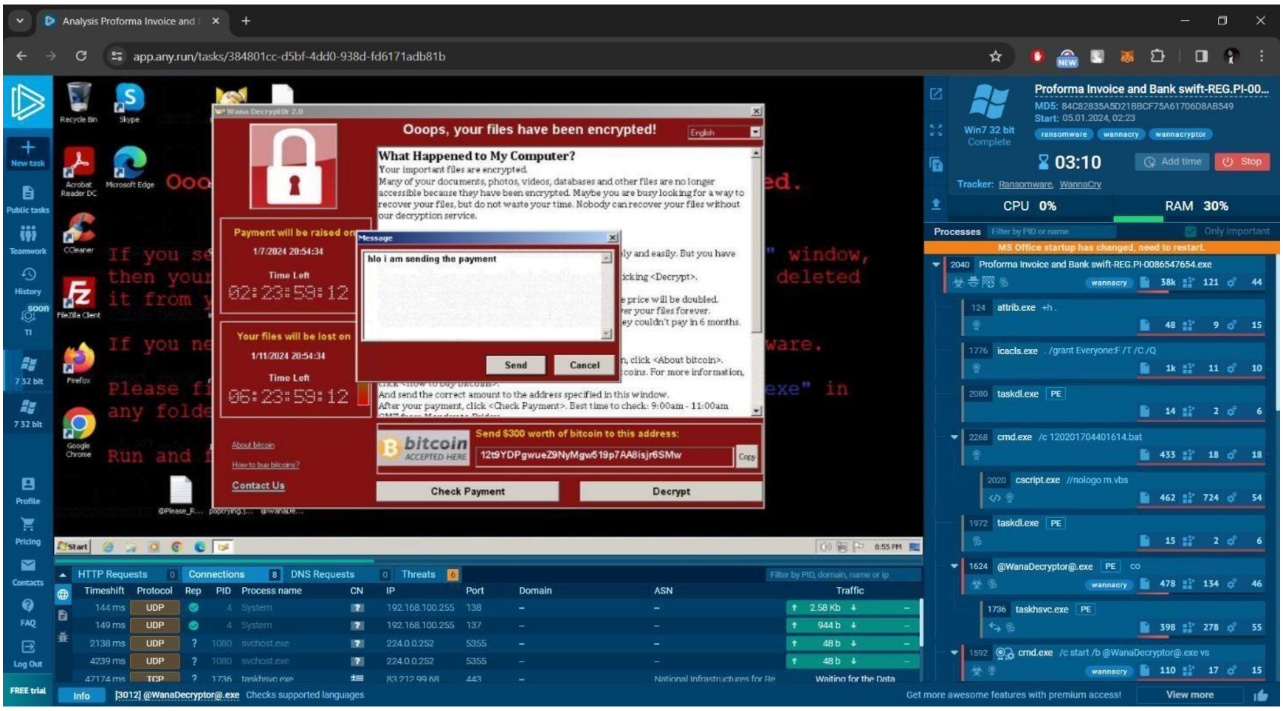
This address has transacted 248 times on the Bitcoin blockchain. It has received a total of 19.69282998 BTC $872,726 and has sent a total of 17.77113037 BTC $787,562 The current value of this address is 1.92169961 BTC $85,163.88

Total Received	Total Sent	Total Volume
19.69282998 BTC $872,726	17.77113037 BTC $787,562	37.46396035 BTC $1,660,288

Proforma Invoice and Bank swift-REG.PI-00...
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 05.01.2024, 02:43
Tracker: Ransomware, WannaCry

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	–	–	604 b
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	–	–	2.79 Kb
588 ms	UDP	?	1080	svchost.exe	?	224.0.0.252	5355	–	–	48 b
3691 ms	UDP	?	1080	svchost.exe	?	224.0.0.252	5355	–	–	48 b

[9] It also had a 'contact us' button on clicking which a popup opens in which we can write a message and sent it to the hackers.



app.any.run/tasks/384801cc-d5bf-4dd0-938d-fd6171adb81b

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Payment will be raised on
1/7/2024 20:54:34
Time Left
02:23:59:12

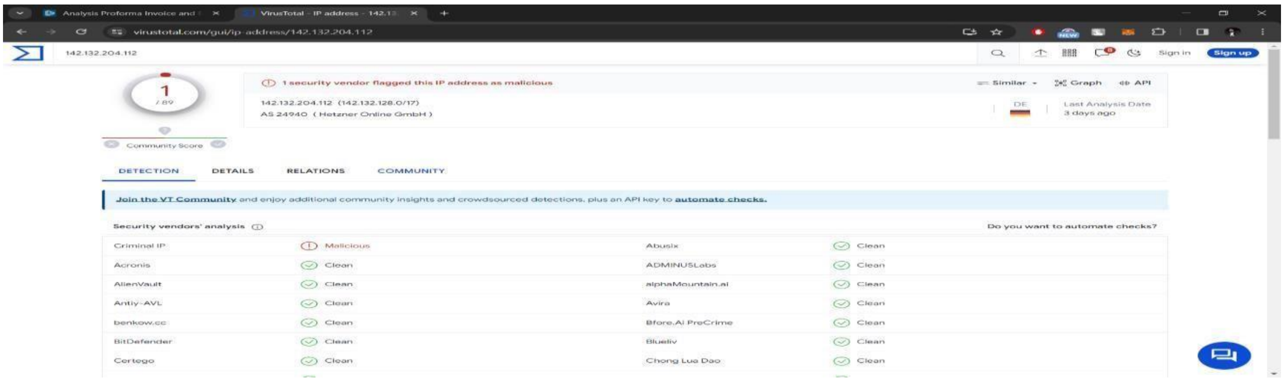
Your files will be lost on
1/11/2024 20:54:34
Time Left
06:23:59:12

Message
hlo i am sending the payment

And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

[10] On pressing the send button it tried to connect to an ip address (142[.]132[.]204[.]112) which was found malicious on virustotal but failed and the wana decryptor 2.0 window was not responding.



virustotal.com/gui/ip-address/142.132.204.112

142.132.204.112

1 / 89

Community Score

1 security vendor flagged this IP address as malicious

142.132.204.112 (142.132.128.0/17)
AS 24940 (Hetzner Online GmbH)

DE

Last Analysis Date
3 days ago

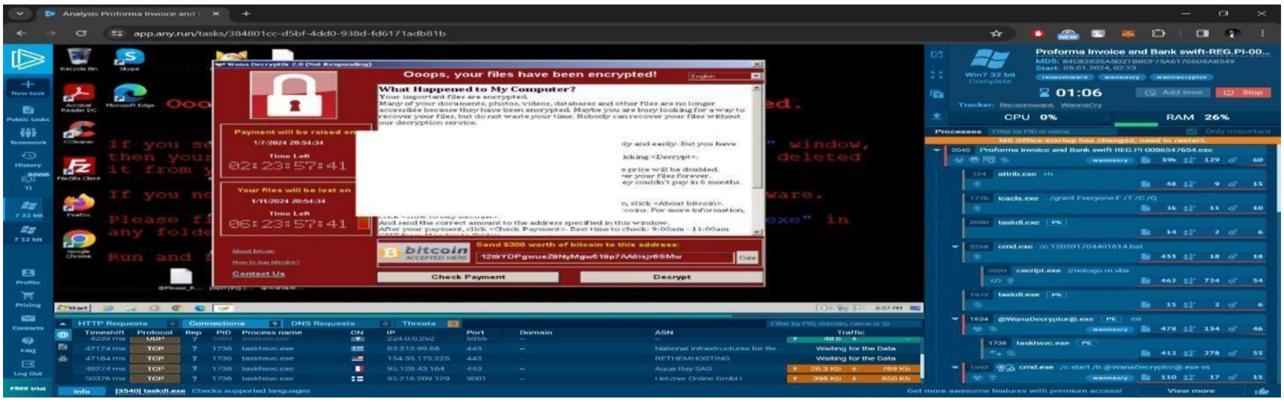
DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Avira	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean



app.any.run/tasks/384801cc-d5bf-4dd0-938d-fd6171adb81b

Wana Decrypt0r 2.0 (Not Responding)

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
1/7/2024 20:54:34
Time Left
02:23:57:41

Your files will be lost on
1/11/2024 20:54:34
Time Left
06:23:57:41

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Proforma Invoice and Bank swift-REG.PI-00...
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 05.01.2024, 02:23
ransomware wannacry wannacryptor
Win7 32 bit Complete
01:06
Tracker: Ransomware, WannaCry
CPU 0% RAM 26%

MS Office startup has changed, need to restart.

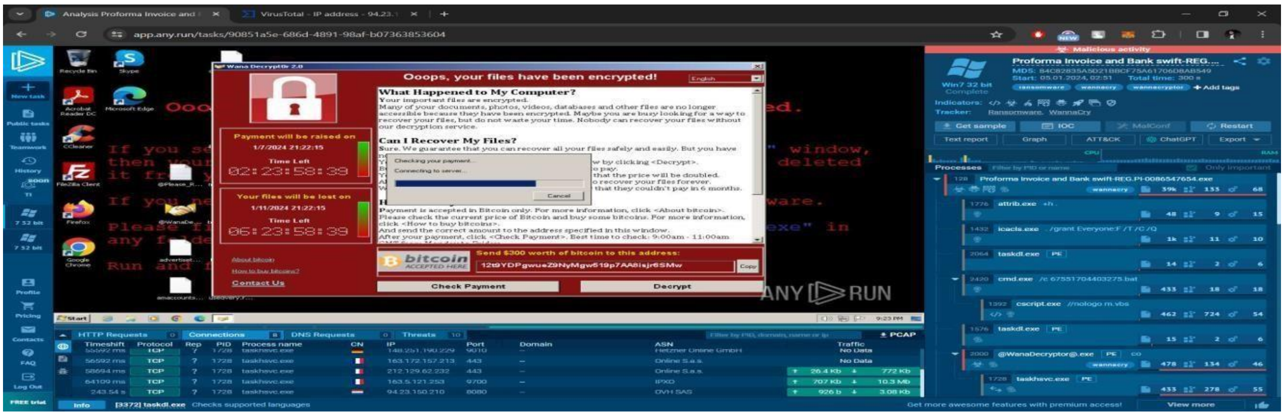
2040 Proforma Invoice and Bank swift-REG.PI-0086547654.exe
124 attrib.exe +h .
1776 icacls.exe . /grant Everyone:F /T /C /Q
2080 taskdl.exe
2268 cmd.exe /c 120201704401614.bat
2020 cscript.exe //nologo m.vbs
1972 taskdl.exe
1624 @WanaDecryptor@.exe
1736 taskhsvc.exe
1092 cmd.exe /c start /b @WanaDecryptor@.exe vs

HTTP Requests 0 | Connections 9 | DNS Requests 0 | Threats

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
4239 ms	UDP	?	1080	svchost.exe		224.0.0.252	5355	—	—	48 b
47174 ms	TCP	?	1736	taskhsvc.exe		83.212.99.68	443	—	National Infrastructures for Re...	Waiting for the Data
47184 ms	TCP	?	1736	taskhsvc.exe		154.35.175.225	443	—	RETHEMHOSTING	Waiting for the Data
48274 ms	TCP	?	1736	taskhsvc.exe		95.128.43.164	443	—	Aqua Ray SAS	26.3 Kb 769 Kb
50376 ms	TCP	?	1736	taskhsvc.exe		95.216.209.129	9001	—	Hetzner Online GmbH	396 Kb 650 Kb

[3540] taskdl.exe Checks supported languages

[11] It also had a check payment button on pressing which it tried to connect to a server for which it tried an ip address (94[.]23[.]150[.]210) which was found malicious on virustotal.



app.any.run/tasks/90851a5e-686d-4891-98af-b07363853604

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have

Checking your payment...
Connecting to server...
Cancel

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
1/7/2024 21:22:15
Time Left
02:23:58:39

Your files will be lost on
1/11/2024 21:22:15
Time Left
06:23:58:39

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Malicious activity

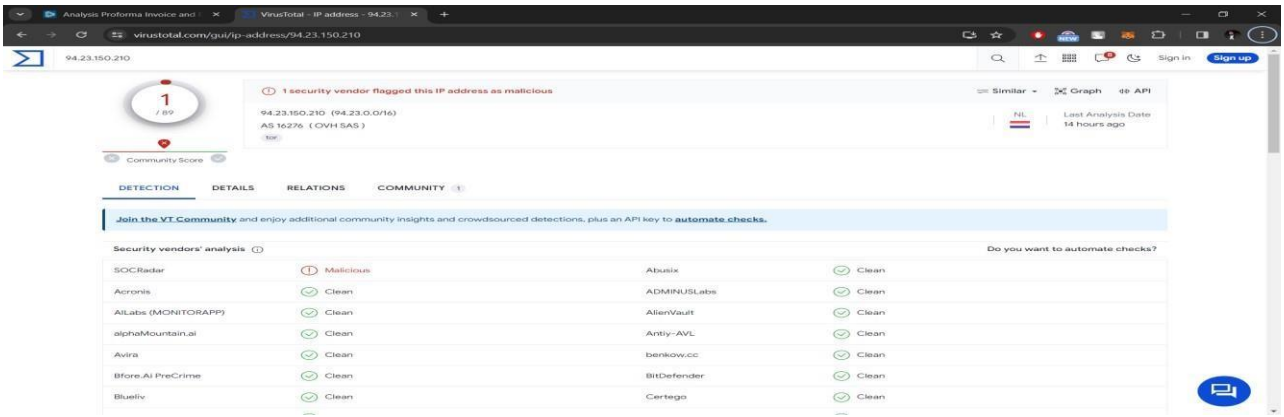
Proforma Invoice and Bank swift-REG....
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 05.01.2024, 02:51 Total time: 300 s
ransomware wannacry wannacryptor
Tracker: Ransomware, WannaCry

128 Proforma Invoice and Bank swift-REG.PI-0086547654.exe
1776 attrib.exe +h .
1432 icacls.exe . /grant Everyone:F /T /C /Q
2064 taskdl.exe
2420 cmd.exe /c 67551704403275.bat
1392 cscript.exe //nologo m.vbs
1576 taskdl.exe
2000 @WanaDecryptor@.exe
1728 taskhsvc.exe

HTTP Requests 0 | Connections 8 | DNS Requests 0 | Threats 10

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
55592 ms	TCP	?	1728	taskhsvc.exe		148.251.190.229	9010	—	Hetzner Online GmbH	No Data
56592 ms	TCP	?	1728	taskhsvc.exe		163.172.157.213	443	—	Online S.a.s.	No Data
58694 ms	TCP	?	1728	taskhsvc.exe		212.129.62.232	443	—	Online S.a.s.	26.4 Kb 772 Kb
64109 ms	TCP	?	1728	taskhsvc.exe		163.5.121.253	9700	—	IPXO	707 Kb 10.3 Mb
243.54 s	TCP	?	1728	taskhsvc.exe		94.23.150.210	8080	—	OVH SAS	926 b 3.08 Kb

[3372] taskdl.exe Checks supported languages



virustotal.com/gui/ip-address/94.23.150.210

94.23.150.210

1 / 89

Community Score

1 security vendor flagged this IP address as malicious

94.23.150.210 (94.23.0.0/16)
AS 16276 (OVH SAS)
tor

NL

Last Analysis Date
14 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

SOCRadar	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Avira	Clean	benkow.cc	Clean
Bfore.Ai PreCrime	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean