Analysis Overview

⚠Request Report Deletion

Submission name:
owo_im_not_ransomware_xd.exe ℹ

Size:
3.4MiB

Type:
peexe (/search?query=filetype:peexe&block_redirect=1) executable (/search?query=filetype:executable&block_redirect=1) ℹ

Mime:
application/x-dosexec

SHA256:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa (/search?query=context:ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa&block_redirect=1)

Operating System:
Windows

Last Anti-Virus Scan:
03/11/2022 22:00:31 (UTC)

Last Sandbox Report:
06/28/2021 15:07:21 (UTC)

malicious

Threat Score: 100/100
AV Detection: 95%
Labeled as: Trojan.Generic (/search?query=vxfamily%3A"Trojan.Generic")

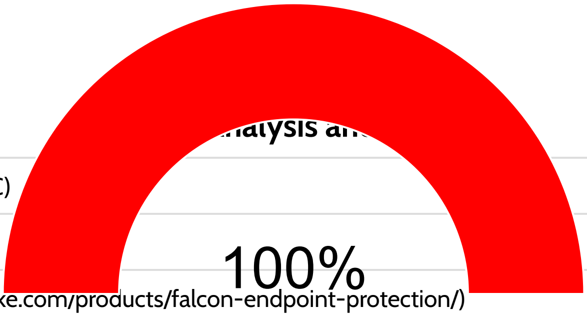
#tag (/search?query=tag%3Atag) #wannacry (/search?query=tag%3Awannacry) #Worm (/search?query=tag%3AWorm) #ransomware (/search?query=tag%3Aransomware) #wanacrypt0r (/search?query=tag%3Awanacrypt0r) #wcry (/search?query=tag%3Awcry) #gozi (/search?query=tag%3Agozi) #isfb (/search?query=tag%3Aisfb) #papras (/search?query=tag%3Apapras) #ursnif (/search?query=tag%3Aursnif)

Link Twitter (/sample-overview/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/share/twitter) E-Mail

Anti-Virus Results

Refresh

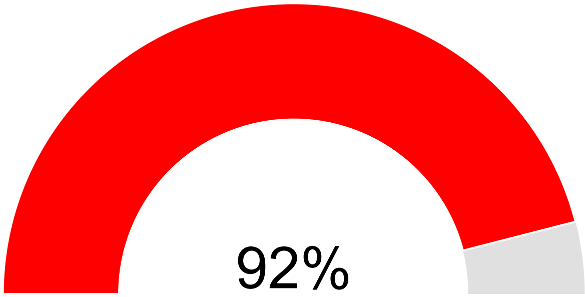
CrowdStrike Falcon



Last Update:	03/11/2022 22:00:31 (UTC)
View Details:	N/A
Visit Vendor:	↗ (https://www.crowdstrike.com/products/falcon-endpoint-protection/)

GET STARTED WITH A FREE TRIAL (https://www.crowdstrike.com/resources/free-trials/try-falcon-prevent/)

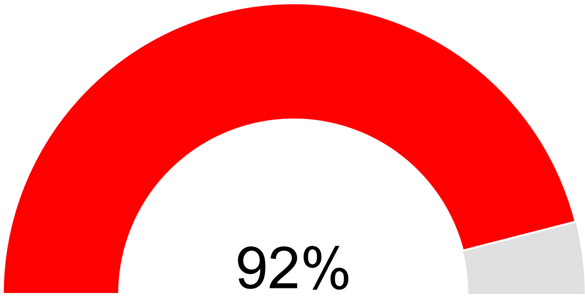
MetaDefender



Multi Scan Analysis

Last Update:	03/11/2022 22:00:31 (UTC)
View Details:	▭
Visit Vendor:	↗ (https://www.opswat.com/metadefender-core?utm_campaign=Technology%%20Partners&utm_source=HA)

VirusTotal



Multi Scan Analysis

Last Update:	03/11/2022 22:00:31 (UTC)
View Details:	↗ (https://www.virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/detection/f-
Visit Vendor:	↗ (https://www.virustotal.com)

Related Hashes

Related files

Name	Sha256	Verdict
wanna707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a.bin (/sample/59a3230782c6d74bcb8ff8bd4101db211f0f9ace82aa2af054915e4133b21cb2)	59a3230782c6d74bcb8ff8bd4101db211f0f9ace82aa2af054915e4133b21cb2	malicious
Ransomware.WannaCry.zip (/sample/707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a)	707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a	malicious
Ransomewaare exe.zip (/sample/7c42f6f0696c1b6954c3aea6136c8e25b2f179922a143984254f00561d53e784)	7c42f6f0696c1b6954c3aea6136c8e25b2f179922a143984254f00561d53e784	malicious
Ransomware.WannaCry.zip (/sample/61a5eed5d3cf4cf0924bac118acf3deffd2ab3a8fc67024f3c35fcc2061e6511)	61a5eed5d3cf4cf0924bac118acf3deffd2ab3a8fc67024f3c35fcc2061e6511	malicious
Ransomware.WannaCry.zip.zip (/sample/c1aeafa14591bbc30cf385e69e13e71438e0c963b3b0de72ede00c7131194478)	c1aeafa14591bbc30cf385e69e13e71438e0c963b3b0de72ede00c7131194478	malicious
Ransomware.WannaCry.zip.zip (/sample/3eadbb62d7b951ebb98effa2e7f617e14bf8b47b0cf20fc43bec272475913d44)	3eadbb62d7b951ebb98effa2e7f617e14bf8b47b0cf20fc43bec272475913d44	malicious

Samples that dropped this file

Name	Sha256	Verdict

Name	Sha256	Verdict
Server.exe (/sample/5c17f43e95f71d09ae9d3a12e5c586eb257d0bf49ce6551709468c4617a0bf8f)	5c17f43e95f71d09ae9d3a12e5c586eb257d0bf49ce6551709468c4617a0bf8f	malicious

File Collections

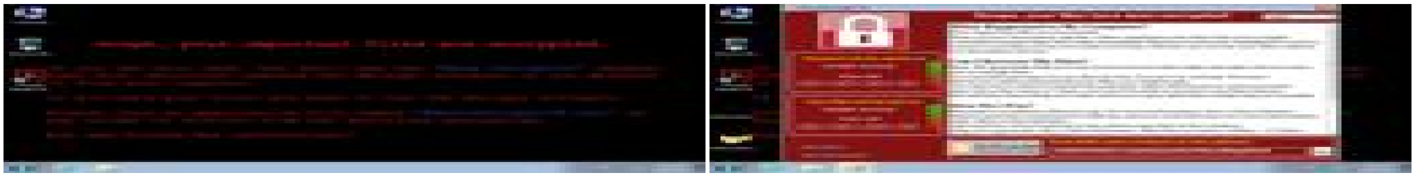
Name	Files number	Verdict
Unknown Files Collection (/file-collection/5d08683d038838f8635349c2)	2	malicious
Unknown Files Collection (/file-collection/5d419b380388389d72762692)	1	malicious
Unknown Files Collection (/file-collection/5d94603d028838392ed04909)	16	malicious
TEST (/file-collection/5dc8e3f8028838e69a830b00)	2	malicious
Unknown Files Collection (/file-collection/5eaefc1f80d8da70db3f7cb7)	32	malicious
Unknown Files Collection (/file-collection/5eaf0022841a2551d02eca79)	27	malicious
Discord fake update and WannaCry (/file-collection/5efc8c4fa89c085d78699c39)	2	malicious
Unknown Files (/file-collection/5fec93599626df54cb66682f)	30	malicious
Unknown Files Collection (/file-collection/61c58abd31d9c446be1a1c75)	15	malicious

Falcon Sandbox Reports

MALICIOUS

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

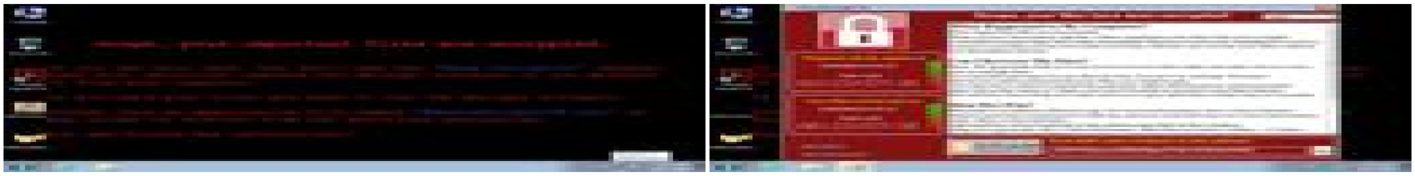
Analyzed on:	06/28/2021 15:07:21 (UTC)
Environment:	Windows 7 32 bit
Threat Score:	100/100
AV Detection:	94% Trojan.Ransom.WannaCryptor
Indicators:	17 36 25
Network:	🇦🇹 🇩🇪 🇫🇷 🇳🇴 🇺🇸



MALICIOUS

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa_abZgnbpWW8.bin

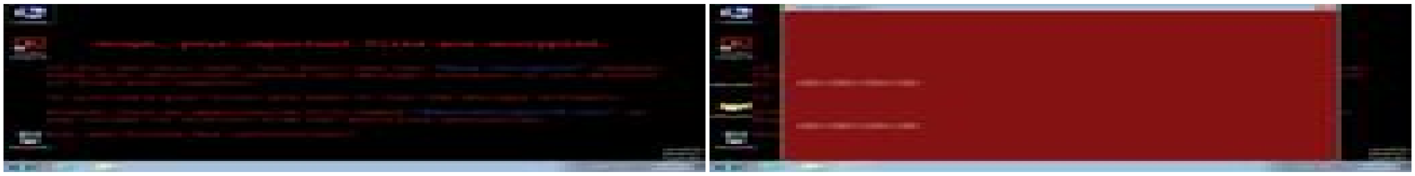
Analyzed on:	06/12/2020 23:39:58 (UTC)
Environment:	Windows 7 32 bit
Threat Score:	100/100
AV Detection:	91% Trojan.Ransom.WannaCryptor
Indicators:	17 34 23
Network:	🇩🇪 🇫🇷 🇭🇺 🇳🇱 🇺🇸



MALICIOUS

owo_im_not_ransomware_xd.exe

Analyzed on:	02/24/2020 16:03:53 (UTC)
Environment:	Windows 7 64 bit
Threat Score:	100/100
AV Detection:	90% Trojan.Ransom.WannaCryptor
Indicators:	14 37 28
Network:	🇩🇪 🇩🇰 🇫🇷 🇬🇧 🇳🇱 🇺🇸



MALICIOUS

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Analyzed on:	08/06/2020 11:08:16 (UTC)
Environment:	Windows 7 32 bit (HWP Support)
Threat Score:	100/100
AV Detection:	90% Trojan.Ransom.WannaCryptor
Indicators:	18 34 24

Network: 🇩🇪 🇪🇺 🇫🇷 🇳🇱 🇷🇴 🇸🇪 🇺🇦 🇺🇸

MALICIOUS

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin

Analyzed on: 08/06/2019 23:46:13 (UTC)

Environment: Android Static Analysis

Threat Score: 100/100

AV Detection: 87% Trojan.Ransom.WannaCryptor

Indicators: 4 0 2

Network: *(none)*

MALICIOUS

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Analyzed on: 06/13/2019 14:15:10 (UTC)

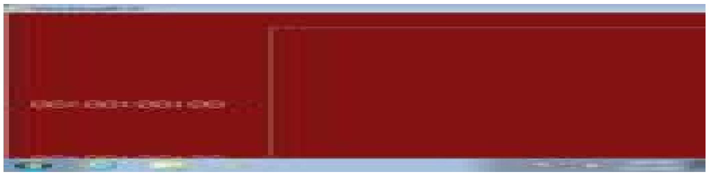
Environment: Windows 7 32 bit (HWP Support)

Threat Score: 100/100

AV Detection: 85% Trojan.Ransom.WannaCryptor

Indicators: 19 43 30

Network: 🇩🇪 🇫🇷 🇬🇧 🇮🇹 🇱🇻 🇳🇱



MALICIOUS

unknownvirus.exe

Analyzed on: 01/29/2020 06:54:06 (UTC)

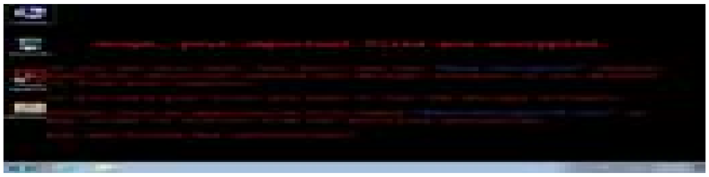
Environment: Linux (Ubuntu 16.04, 64 bit)

Threat Score: 100/100

AV Detection: 81% Trojan.Ransom.WannaCryptor

Indicators: (17) (40) (27)

Network: 🇨🇭 🇨🇿 🇩🇪 🇫🇷 🇳🇱



Incident Response

Risk Assessment

Remote Access

Reads terminal service related keys (often RDP related)

Ransomware

Deletes volume snapshots (often used by ransomware)
Detected indicator that file is ransomware

Spyware

Contains ability to open the clipboard
Deletes volume snapshots (often used by ransomware)

Persistence

Disables startup repair
Grants permissions using icacls (DACL modification)
Spawns a lot of processes
Tries to suppress failures during boot (often used to hide system changes)
Writes data to a remote process

Fingerprint

Queries kernel debugger information
Queries process information
Reads system information using Windows Management Instrumentation Commandline (WMIC)

Reads the active computer name
Reads the cryptographic machine GUID

Evasive

Marks file for deletion
Possibly checks for the presence of an Antivirus engine

Network Behavior

Contacts 48 hosts. 🔍 View all details

MITRE ATT&CK™ Techniques Detection

We found MITRE ATT&CK™ data in 6 reports, on average each report has 31 mapped indicators.
🔍 View all details

Community

Anonymous commented 5 months ago

WC

Anonymous commented 6 months ago

proyecto escolar

48 comments are hidden. Please click this link to display all.

❗ You must be logged in (/login) to submit a comment.