Goodwill ransomware group propagates very unusual demands in exchange for the decryption key. The Robin Hood-like group is forcing its Victims to donate to the poor and provides financial assistance to the patients in need.

Category: Malware Intelligence Type/Family: Ransomware Industry: Multiple Region: Global

Executive Summary

- CloudSEK's Threat Intelligence Research team has recently analyzed GoodWill ransomware.
- The ransomware group propagates very unusual demands in exchange for the decryption key. The Robin Hood-like group claims to be interested in helping the less fortunate, rather than extorting victims for financial motivations.
- The group's multiple-paged ransom note suggests that victims perform three socially driven activities to be able to download the decryption key.
- CloudSEK researchers have identified certain artefacts of the threat group that indicate direct attribution to India.

GoodWill ransom note page that explains the group's aimGoodWill ransom note page that explains the group's aim
GoodWill ransom note page that explains the group's aim

Analysis and Attribution for GoodWill Ransomware

Features of the GoodWill Ransomware

GoodWill ransomware was identified by CloudSEK researchers in March 2022. As the threat group's name suggests, the operators are allegedly interested in promoting social justice rather than conventional financial reasons. CloudSEK researchers have been able to identify the following features of GoodWill:

- The ransomware is written in .NET and packed with UPX packers.
- It sleeps for 722.45 seconds to interfere with dynamic analysis.
- It leverages the AES_Encrypt function to encrypt, using the AES algorithm.
- One of the strings is "GetCurrentCityAsync," which tries to detect the geolocation of the infected device.

Once infected, the GoodWill ransomware worm encrypts documents, photos, videos, databases, and other important files and renders them inaccessible without the decryption key. The actors suggest that victims perform three socially driven activities in exchange for the decryption key:

- Activity 1: Donate new clothes to the homeless, record the action, and post it on social media.

GoodWill Ransomware : Image of Activity 1 described in detailGoodWill Ransomware : Image of Activity 1 described in detail
GoodWill Ransomware : Image of Activity 1 described in detail

- Activity 2: Take five less fortunate children to Dominos, Pizza Hut or KFC for a treat, take pictures and videos, and post them on social media.

GoodWill Ransomware : Image of Activity 2 described in detailGoodWill Ransomware : Image of Activity 2 described in detail
GoodWill Ransomware: Image of Activity 2 described in detail

- Activity 3: Provide financial assistance to anyone who needs urgent medical attention but cannot afford it, at a nearby hospital, record audio, and share it with the operators.

GoodWill Ransomware : Image of Activity 3 and details of acquiring the decryption kitGoodWill Ransomware : Image of Activity 3 and details of acquiring the decryption kit
GoodWill Ransomware : Image of Activity 3 and details of acquiring the decryption kit

- The ransomware group demands that the victims record each activity and mandatorily post the images, videos, etc. on their social media accounts.
- Once all three activities are completed, the victims should also write a note on social media (Facebook or Instagram) on "How you transformed yourself into a kind human being by becoming a victim of a ransomware called GoodWill."
- Since there are no known victims/ targets for the ransomware group, their Tactics, Techniques and Procedures remain unknown.

How to Acquire the Decryption Kit for GoodWill Ransomware

Upon completing all three activities, the ransomware operators verify the media files shared by the victim and their posts on social media. The actor will then share the complete decryption kit which includes the main decryption tool, password file and a video tutorial on how to recover all important files.

Information from Open Source

- Our researchers were able to trace the email address, provided by the ransomware group, back to an Indian based IT security solutions & services company, that provides end-to-end managed security services.
- On analyzing the ransomware, CloudSEK threat intelligence researchers extracted the strings of GoodWill:
    - There are some 1246 strings of this ransomware, out of which 91 strings overlap with the HiddenTear ransomware.
    - HiddenTear is an open-source ransomware developed by a Turkish programmer and its PoC was then released on GitHub. GoodWill operators may have gained access to this allowing them to create a new ransomware with necessary modifications.
    - CloudSEK researchers found the following strings of the malware interesting:
        - "error hai bhaiya": This string is written in Hinglish, which means "there is an error, brother." This indicates that the operators are from India and that they speak Hindi.
- - ".gdwill": This string indicates that the file extension used by the ransomware on encrypting files is .gdwill.
- The following network artifacts, associated with GoodWill, were discovered by our researchers. These are GoodWill ransomware tunnels that are also subdomains of Ngrok.io:
    - http://9855-13-235-50-147(.)ngrok(.)io/ (Dashboard of GoodWill ransomware)
    - http://9855-13-235-50-147(.)ngrok(.)io/alertmsg(.)zip
    - http://9855-13-235-50-147(.)ngrok(.)io/handshake(.)php
    - http://84a2-3-109-48-136(.)ngrok(.)io/kit(.)zip

Dashboard of GoodWill ransomware group as directed from http://9855-13-235-50-147(.)ngrok(.)ioDashboard of GoodWill ransomware group as directed from http://9855-13-235-50-147(.)ngrok(.)io
Dashboard of GoodWill ransomware group as directed from http://9855-13-235-50-147(.)ngrok(.)io

Dashboard of GoodWill ransomware group Dashboard of GoodWill ransomware group
Dashboard of GoodWill ransomware group

- As shown above, the IP addresses 3.109.48.136 and 13.235.50.147 are provided as subdomains in the URL. On a detailed investigation, our researchers discovered that both IP addresses are located in Mumbai, India.

IP information on 3.109.48.136 and 13.235.50.147IP information on 3.109.48.136 and 13.235.50.147
IP information on 3.109.48.136 and 13.235.50.147

Impact & Mitigation

Impact	Mitigation
• The exposed confidential details could reveal business practices and intellectual property. • It could also result in temporary, and possibly permanent, loss of company data. • A possible shutdown of the company's operations and accompanied revenue loss. • Financial loss associated with remediation efforts. • Damage to the company's reputation. • Potential account takeovers. • Criminals could use personal data such as name, date of birth, address etc., in tandem with social engineering and identity theft.	• Audit and monitor event and incident logs to identify unusual patterns and behaviors. • Implement security configurations on network infrastructure devices such as firewalls and routers. • Enable tools and applications that prevent malicious programs from being executed. • Reset compromised user login credentials and implement a strong password policy. • Enforce data protection, backup, and recovery measures. • Implement multifactor authentication across devices and platforms. • Perform security skills assessment and training for all personnel regularly. • Conduct periodic red-team exercises and penetration tests. • Monitor for anomalies, in user accounts and systems, that could be indicators of possible takeovers.

Indicators of Compromise (IoCs)

- MD5: cea1cb418a313bdc8e67dbd6b9ea05ad
- SHA-1: 8d1af5b53c6100ffc5ebbfbe96e4822dc583dca0
- SHA-256: 0facf95522637feaa6ea6f7c6a59ea4e6b7380957a236ca33a6a0dc82b70323c
- Vhash: 27503675151120c514b10412
- Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

References

- #https://en.wikipedia.org/wiki/Traffic_Light_Protocol

Appendix

Introduction message on initiating the ransomware attackIntroduction message on initiating the ransomware attack
Introduction message on initiating the ransomware attack

Introduction to GoodWill ransomwareIntroduction to GoodWill ransomware
Introduction to GoodWill ransomware

Image explaining how the victim can submit proof of their activitiesImage explaining how the victim can submit proof of their activities
Image explaining how the victim can submit proof of their activities

Photo frame provided on completion of all activitiesPhoto frame provided on completion of all activities
Photo frame provided on completion of all activities

Press Mentions

This Report was mentioned in

- New virus forces people to donate to the poor if they want their data recovered | https://metro.co.uk/2022/05/24/new-ransomware-demands-victims-donate-to-the-poor-to-unlock-their-data-16698304/ | Metro UK - 24 May 2022
- New ransomware makes victim donate to poor, financial help to needy patients | https://economictimes.indiatimes.com/tech/technology/new-ransomware-makes-victim-donate-to-poor-financial-help-to-needy-patients/articleshow/91726417.cms | Economic Times Tech - May 22, 2022
- Cyber crime or forced charity? ‘Goodwill’ ransomware makes victim donate to poor, financial help to needy patients | https://www.financialexpress.com/industry/technology/cyber-crime-or-forced-charity-goodwill-ransomware-makes-victim-donate-to-poor-financial-help-to-needy-patients/2533802/ | Financial Express - May 22,2022
- New 'GoodWill' ransomware makes targets donate to poor, provide financial help to needy patients | https://www.cnbctv18.com/information-technology/new-goodwill-ransomware-victim-donate-poor-financial-help-needy-patients-cloudsek-13583332.htm | CNBCTv 18 - May 23, 2022
- GoodWill ransomware detected in India makes victim donate to poor, provides financial help to needy patients | https://www.businessinsider.in/tech/news/goodwill-ransomware-detected-in-india-makes-victim-donate-to-poor-provides-financial-help-to-needy-patients/amp_articleshow/91736850.cms | Business Insider - May 23, 2022
- Goodwill ransomware wants you to help needy people to get a decryption key | https://www.bgr.in/news/goodwill-ransomware-wants-you-to-help-needy-people-to-get-decryption-key-1274011/ | BGR India - May 23,2022

Table of Contents

Try XVigil for free

Request an easy and customized demo for free