Sakarya University Journal of Science

ISSN : 2147-835X
Publisher : Sakarya University

Vol. 28, No. 4, 774-781, 2024
DOI: https://doi.org/10.16984/saufenbilder.1442756

Research Article

Analyzing TorrentLocker Ransomware Attacks: A Real Case Study

İlker Kara[1,2]

[1] Cankiri Karatekin University, Department of Faculty of Engineering, Electronics and Computer Engineering, Çankırı, Türkiye, karaikab@gmail.com
[2] Cankiri Karatekin University, Department of Medical Services and Techniques, Çankırı, Türkiye

ARTICLE INFO

Keywords:
Ransomware
TorrentLocker
Cybersecurity

Article History:
Received: 25.02.2024
Accepted: 02.07.2024
Online Available: 01.08.2024

ABSTRACT

Ransomware is malicious software that targets computers, mobile phones, tablets, and other digital devices. These types of software typically encrypt files on the target device, blocking access, and then demand a ransom. TorrentLocker attacks have become particularly popular in recent years, emerging as prominent threats in the realm of cybersecurity. TorrentLocker poses a serious threat to the digital data of users and organizations, exacerbating the financial and reputational damages stemming from cyberattacks. This study provides a framework to understand the target audience, attack strategies, and operations of TorrentLocker ransomware. Conducted through a real case analysis, this examination sheds light on the TorrentLocker attack strategy and elucidates the tracing and identification of the attacker post-attack. The aim of this study is to raise awareness among cybersecurity professionals, organizations, and individual users about TorrentLocker ransomware attacks, aiming to prevent such attacks and track down traces left by the attacker's post-incident. This detailed analysis of TorrentLocker ransomware attacks serves as a crucial resource to enhance protection against future ransomware attacks and contributes to the body of work in this field.

1. Introduction

In today's cybersecurity landscape, ransomware attacks have emerged as a growing threat [1]. With technological advancements and the increasing digitization of our world, cybercriminals' attack methods and techniques have become increasingly complex and sophisticated. Ransomware can inflict serious damage on the digital data of individual users and organizations, raising significant concerns in terms of cybersecurity [2]. The growing frequency and sophistication of these attacks demonstrate that this threat can have far-reaching consequences, not only affecting individuals but also impacting businesses, public institutions, and critical infrastructure. In this context, developing a deeper understanding of ransomware and establishing effective defense strategies are of critical importance in combating today's complex cyber threats. According to the AV-Test Institute report, as of 2024, 950 million new malware were released [3]. The countries where these attacks have been most prevalent include Canada, Australia, and New Zealand, targeting users in these regions [4]. The victims have paid the attackers a ransom amounting to US$585,401 in Bitcoins [4].

TorrentLocker stands out among ransomware and is a malicious software targeting computer users. This software infiltrates computer systems, encrypting files to block user access and then demands a ransom to decrypt the files unless paid. Ransomware attacks like TorrentLocker represent a milestone in the evolution of ransomware. Historically, ransomware attacks were documented with the emergence of the malicious software known as AIDS Trojan (PC Cyborg) in 1989 [5]. However, the widespread adoption and sophistication of modern ransomware began to be observed in the early

Cite as: İ. Kara (2024). Analyzing TorrentLocker Ransomware Attacks: A Real Case Study, *Sakarya University Journal of Science*, 28(4), 774-781. https://doi.org/10.16984/saufenbilder.1442756

2000s. TorrentLocker, emerged in 2014, rapidly spreading as a prominent example of ransomware [6]. This period marked the significant rise of ransomware in the cybercrime arena and the development of various tactics. In this context, TorrentLocker and similar ransomware attacks serve as noteworthy examples of cybercriminals adopting complex and sophisticated attack strategies in cyberspace [7-11].

The infection of TorrentLocker ransomware is primarily facilitated through a variety of mechanisms including social engineering tactics, phishing emails, counterfeit software updates, and downloads. These malware programs deceive users with seemingly official, yet harmful links or attachments contained in messages or emails, leading to the malware infecting their devices when these links are clicked or attachments are opened. Moreover, the ransomware is capable of disseminating through the exploitation of security vulnerabilities and via the distribution of harmful files on widely used file-sharing platforms or cloud storage services.

Research on topics such as the origins of ransomware, propagation methods, encryption algorithms, and ransom payment systems contributes to understanding this threat and determining effective countermeasures. Therefore, the importance of research in this area is increasing. The findings of these studies can assist policymakers in cybersecurity, companies, and individuals in developing more effective protection strategies against such attacks.

This study focuses on a real case analysis and examination of TorrentLocker, one of the most significant examples in the field, to investigate the attack strategy and analysis methods of ransomware. Additionally, this case analysis provides an important contribution to understanding how ransomware operates in the real world and prepares against future attacks.

2. Related Work

Ransomware and particularly real-life case analyses have been a significant focal point in cybersecurity research. Numerous academic studies have examined the prevalence, operation mechanisms, and impacts of ransomware. This section focuses on significant developments of ransomware throughout history.

In 2013, the emergence of Cryptolocker ransomware marked another significant development in the landscape of cyber threats. Characterized by its propagation through infected email attachments, Cryptolocker operated by encrypting victim files using the RSA encryption method. Victims were then coerced into paying ransom using digital currencies, notably Bitcoin, in exchange for the decryption key. Furthermore, attackers threatened to delete the private encryption key unless payment was made before a specified deadline.

While initial ransomware attacks predominantly targeted Windows operating systems, a notable shift occurred in 2015 when Fusob emerged, specifically targeting mobile devices, with attacks persisting until March 2016 [4]. Similar to its predecessors, Fusob employed intimidation tactics to coerce victims into paying ransom. Concurrently, TeslaCrypt Mukesh, active from 2015 to 2016, propagated through email and targeted specific system libraries such as ole32dir.dll, kernel32.dll, and apphelp.dll. Furthermore, it encrypted various file types including game files and special files (.doc, .pdf, .py, .ptx, .jpeg, etc.). However, in May 2016, the threat was neutralized with the release of the primary decryption key by the attackers [4].

In the subsequent year, 2021, the frequency of attacks surged to an alarming rate, averaging one attack every 11 seconds [12]. Beginning in 2012, the spread of Reveton ransomware marked a significant development in the realm of cyber threats. Distinguished from Xorist, Reveton employed intimidation tactics to coerce victims into paying ransoms. For instance, victims received threats indicating that their access had been logged in an illicit area, with law enforcement intervention imminent unless the ransom was paid. Furthermore, victims were compelled to comply with ransom demands by being informed that their IP addresses had been identified, accompanied by claims of capturing actual webcam footage. Payment of the ransom was mandated through the use of MoneyPak cards.

In another study, ransomware continues to pose a significant threat by infiltrating victim systems through various means, typically encrypting files and demanding a ransom for decryption [13]. Despite the development of security measures such as firewalls, antivirus programs, and automated analysis tools to counter this threat, they have shown limited success in safeguarding valuable assets stored in both local and cloud storage resources. In response to this challenge, this study proposes an effective method for detecting and analyzing ransomware attacks, which is discussed in detail through a case study. Through the application of the proposed method, the study reveals insights into the characteristic behavior of the Onion ransomware, offering potential avenues for identifying attackers. Furthermore, this paper provides a comprehensive overview of the methods and techniques utilized in detecting and analyzing ransomware attacks, shedding light on the evolving landscape of this cybersecurity threat.

3. Materials and Methods

The TorrentLocker ransomware attacks typically occur through the dissemination of infected files via email. When users open these files, the ransomware infects their systems and begins encrypting files. Once the encryption process is complete, users lose access to their files, and a ransom demand is issued. In this section, we introduce a case example prepared for TorrentLocker ransomware attacks and the business computer and analysis tools used in the analysis.

3.1. Dataset

In case analysis studies, it is crucial that the selected sample is up-to-date and fully encompasses the problem at hand. To achieve this, collaboration was established with the information security department of companies operating in Turkey to utilize one of the latest examples for this purpose.

3.2. Preparation of analysis environment

All analyses were conducted on a Lenovo V530 Intel Core i7 7500U workstation. The workstation was equipped with 128 GB of RAM and a 512 GB SSD. It operated on the Windows 10 Pro operating system.

The analyses were performed using "AccessData Forensic Toolkit v6.3.0.186 (Free version)" and "Wireshark 3.4.3 (Free version) 49.2". As the analyzed sample is a real cyber attack and forensic case, some information is presented with blur for confidentiality purposes.

3.3. Preparation of analysis environment

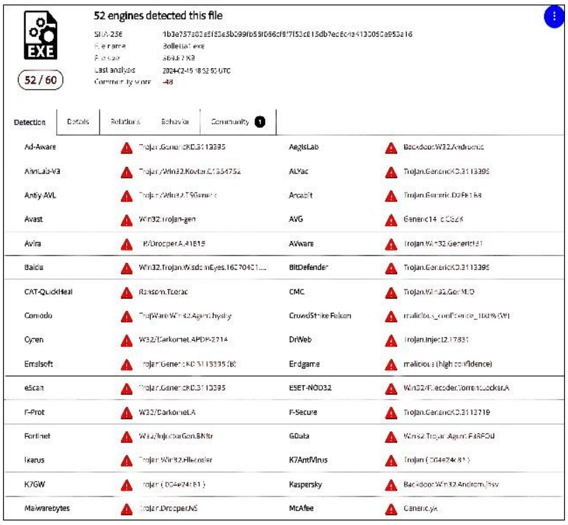
The examination of digital material was conducted using forensic practices within the framework of Digital Forensics, ensuring data integrity by writing protection (Write Blocker), and in compliance with international standards. Forensic copies were created using AccessData Forensic Toolkit program (Table 1).

Table 1. Image information of victim system

Description	Physical Disk, 967.373.186 Sectors 456,8 GB
Total Size	500.170.862.166 Bytes (456,8 GB)
Total Sectors	967.373.186
Acquisition MD5	953839c2a763adbce05a61f53f8ac988
Verification MD5	953839c2a763adbce05a61f53f8ac988
Acquisition SHA1	8acd345afecd3798763ca7dcb 166f5f78acd483c
Verification SHA1	8acd345afecd3798763ca7dcb 166f5f78acd483c

During the investigation, the internet history and suspicious activities on the target computer's last usage dates were examined. It was noted that the file named "TURKCELL_eFATURA.exe" was present during the recent activities, prompting a closer inspection of this suspicious file. The file "TURKCELL_eFATURA.exe" was initially queried on the website www.virustotal.com, which aggregates database information from 60 antivirus firms (Figure 1).

Upon thorough examination, it was determined that the suspicious file is a type of malicious software known as "TorrentLocker," a form of ransomware that encrypts users' personal files.



52 engines detected this file

52 / 60

SHA-256	1b3e757a83a5f83a5b099fb55f066cf8f7f53c815db7ec6c4a4130050a953a16
File name	Bolletta1.exe
File size	369.87 KB
Last analysis	2024-02-15 18:32:50 UTC
Community score	-48

Ad-Aware	Trojan.GenericKD.3113395	AegisLab	Backdoor.W32.Andromeda
AhnLab-V3	Trojan/Win32.Kovter.C1354752	ALYac	Trojan.GenericKD.3113395
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Trojan.Generic.D2FB1B3
Avast	Win32:Trojan-gen	AVG	Generic14.c.C62K
Avira	TR/Dropper.A.41815	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Trojan.GenericKD.3113395
CAT-QuickHeal	Ransom.Teerac	CMC	Trojan.Win32.Gen!O
Comodo	TrojWare.Win32.Agent.hyshy	CrowdStrike Falcon	malicious_confidence_100% (W)
Cyren	W32/Darkomet.APDP-2714	DrWeb	Trojan.Inject2.17831
Emsisoft	Trojan.GenericKD.3113395 (B)	Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.3113395	ESET-NOD32	Win32/Filecoder.TorrentLocker.A
F-Prot	W32/Darkomet.A	F-Secure	Trojan.GenericKD.3113719
Fortinet	W32/InjectorGen.BN!tr	GData	Win32.Trojan.Agent.F8RFOU
Ikarus	Trojan.Win32.Filecoder	K7AntiVirus	Trojan (004e24c81)
K7GW	Trojan (004e24c81)	Kaspersky	Backdoor.Win32.Androm.jlsv
Malwarebytes	Trojan.Dropper.NS	McAfee	Generic.yk

Figure 1. Screenshot of the query the www.virustotal.com website

Table 2. Image information of victim system

File Name	TURKCELL_eFATURA.exe
Change Date	15.02.2024 16:34:54 (2024-02-15 33:34:54 UTC)
File Size	378.749 bytes (369,9 KB)
Value of MD5	a1e75907b75ccf086882d 7a01e0599e6
File Path	IMAGE.001/Partition 1/NONAME [NTFS]/[root]/RECYCLER/S-1-5-21-1417001333-261478967-682003330-1003/Dc234.zip»TURKCELL_eFATURA.exe

Upon detecting the encryption of personal files on the victim computer through the malicious software described in Table 2, an examination of file-directory and registry movements associated with this malicious software was conducted (Table 2).

As seen in Table 3, the "TURKCELL_eFATURA.exe" file initiates a process of creating itself under the Windows/temp folder. Subsequently, a file named "vssadmin.exe" is created in the system32 directory of the Windows system. This tactic is employed to prevent the detection and removal of the ransomware. Following this stage, when the "TURKCELL_eFATURA.exe" file is executed, it triggers a series of processes on your computer, including the encryption of files.

Table 3. Infiltration process of the "TURKCELL_eFATURA.exe" TorrentLocker file into the victim computer

Creates process:	**C:\windows\temp\TURKCELL eEATURA.exe {C:\windows\temo\TURKCELL eEATURA.exe"}**
Creates process:	C:\windows\SysW0W64\explorer.exe {"C:\Windows\system32\explorer.exe"}
Creates process:	C:\windows\SysWOW66\vssadmin.exe {vsseanin.exe Delete Shedows /All /Quiet}
Loads service:	ProtectedStorage [C:\windows\system32\1sass.exe]
Reads from process:	PID:1548 C:\windows\ Temp\TURKCELL_eFATURA.exe
Writes to process:	PID:1548 C:\windows\Temp\TURKCELL_eFATURA.exe
Writes to process:	PID:1724 C:\windowg\SysW0W64\explorer.exe
Terminates process:	C:\windows\Temp\TURKCELL_eFATURA.exe
Terminates process:	C:\windows\Temp\TURKCELL_eFATURA.exe

To examine this activity in more detail, Windows registry movements were investigated (Table 4).

Table 4. Windows registry movements of the "TURKCELL_eFATURA.exe" TorrentLocker file

Creates key:	**HKLM\ software\microsoft\windows\currentversion \run**
Creates key:	HKLM \software\ microsoft \windous\currentversion\internet settings
Creates key:	HKLM \software\microsoft\internet explorer\phishingfilter
Creates key:	HKLM\ software\wor6432node\ microsoft \tracing
Deletes value:	HKCU\ softwere\microsoft\windows\currentversion\internet sectings[proxyserver]
Sets/Creates value:	**HKLM\ microsoft\software\windows\currentversion\run{ucerepat}**
Sets/Creates value:	HKLM\ microsoft\internetexploler\ phishingfilter \{enebledv9}

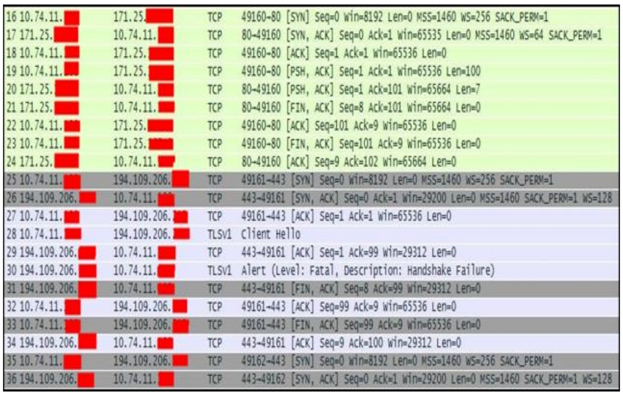
After infiltrating the computer by TorrentLocker, such as the "TURKCELL_eFATURA.exe" file, various changes have been made in the Windows registry. These changes are typically made to enable the ransomware to operate more effectively or to make it difficult for the user to use their computer. When examining Table 3, it is observed that the "TURKCELL_eFATURA.exe" file, a TorrentLocker file, has created startup entries in the Windows registry to automatically start at the computer's boot. This allows the "TURKCELL_eFATURA.exe" TorrentLocker ransomware to run automatically every time the system starts, making it difficult for the user to notice.

The "windows\currentversion\run" registry entry contains a list of programs that will automatically run at the startup of the Windows operating system. As a ransomware, TorrentLocker aims to use this registry entry to automatically start itself at computer boot. This registry entry typically contains a list of programs that will run when the user opens their computer in the current session. Therefore, by using this entry, ransomware can stealthily start itself at computer boot, making it difficult for the user to notice. This tactic enables the ransomware to continuously operate, performing tasks such as encrypting files and displaying the ransom note.

The creation of such a registry entry can enable the "TURKCELL_eFATURA.exe" TorrentLocker ransomware to operate more effectively. However, users can monitor such automatic startup entries and remove unnecessary or malicious entries.

Following the examination of file, directory, and registry movements, the network movements of the "TURKCELL_eFATURA.exe" TorrentLocker ransomware were investigated using Wireshark software. The obtained data allows for the analysis of network traffic. These network analyses provide an opportunity to thoroughly examine the interactions of TorrentLocker ransomware with computer systems. The examination of data recorded through Wireshark allows us to determine how the ransomware communicates with target systems, which network protocols it uses, and what types of data are being transferred.

These analyses have helped us develop a deeper understanding of the impact and propagation strategies of TorrentLocker ransomware. Additionally, examining the network traffic data recorded through Wireshark allows for tracing the footprint of the attacker in case the ransomware communicates with the attacker (Figure 2).



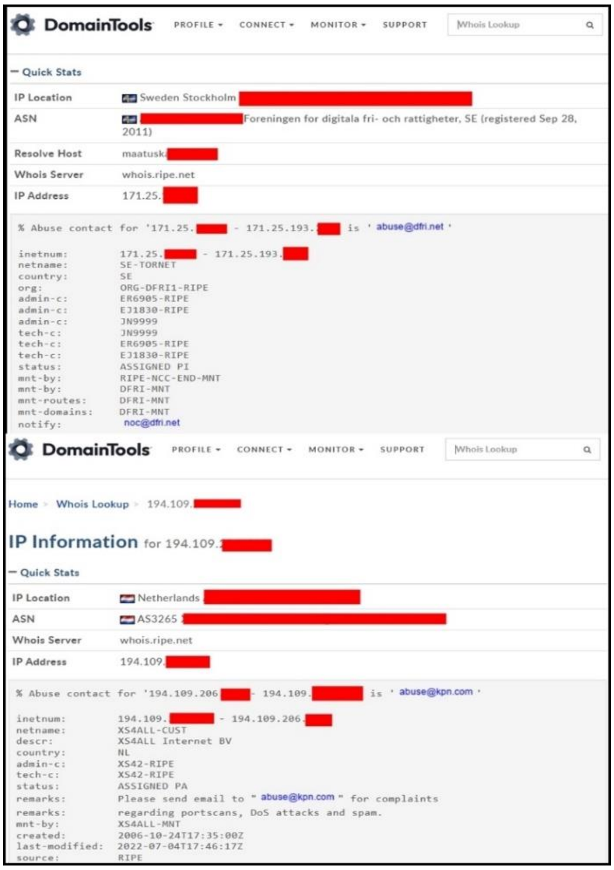
```
16 10.74.11.[redacted]     171.25.[redacted]      TCP    49160→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17 171.25.[redacted]       10.74.11.[redacted]    TCP    80→49160 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
18 10.74.11.[redacted]     171.25.[redacted]      TCP    49160→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
19 10.74.11.[redacted]     171.25.[redacted]      TCP    49160→80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=100
20 171.25.[redacted]       10.74.11.[redacted]    TCP    80→49160 [PSH, ACK] Seq=1 Ack=101 Win=65664 Len=7
21 171.25.[redacted]       10.74.11.[redacted]    TCP    80→49160 [FIN, ACK] Seq=8 Ack=101 Win=65664 Len=0
22 10.74.11.[redacted]     171.25.[redacted]      TCP    49160→80 [ACK] Seq=101 Ack=9 Win=65536 Len=0
23 10.74.11.[redacted]     171.25.[redacted]      TCP    49160→80 [FIN, ACK] Seq=101 Ack=9 Win=65536 Len=0
24 171.25.[redacted]       10.74.11.[redacted]    TCP    80→49160 [ACK] Seq=9 Ack=102 Win=65664 Len=0
25 10.74.11.[redacted]     194.109.206.[redacted] TCP    49161→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26 194.109.206.[redacted]  10.74.11.[redacted]    TCP    443→49161 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
27 10.74.11.[redacted]     194.109.206.[redacted] TCP    49161→443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
28 10.74.11.[redacted]     194.109.206.[redacted] TLSv1  Client Hello
29 194.109.206.[redacted]  10.74.11.[redacted]    TCP    443→49161 [ACK] Seq=1 Ack=99 Win=29312 Len=0
30 194.109.206.[redacted]  10.74.11.[redacted]    TLSv1  Alert (Level: Fatal, Description: Handshake Failure)
31 194.109.206.[redacted]  10.74.11.[redacted]    TCP    443→49161 [FIN, ACK] Seq=8 Ack=99 Win=29312 Len=0
32 10.74.11.[redacted]     194.109.206.[redacted] TCP    49161→443 [ACK] Seq=99 Ack=9 Win=65536 Len=0
33 10.74.11.[redacted]     194.109.206.[redacted] TCP    49161→443 [FIN, ACK] Seq=99 Ack=9 Win=65536 Len=0
34 194.109.206.[redacted]  10.74.11.[redacted]    TCP    443→49161 [ACK] Seq=9 Ack=100 Win=29312 Len=0
35 10.74.11.[redacted]     194.109.206.[redacted] TCP    49162→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
36 194.109.206.[redacted]  10.74.11.[redacted]    TCP    443→49162 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
```

Figure 2. Network movements recorded with Wireshark for the "TURKCELL_eFATURA.exe" file

Upon analyzing the network traffic of the "TURKCELL_eFATURA.exe" TorrentLocker ransomware, it was observed that it attempted to communicate with the IP addresses "171.25.XXX.X" and "194.109.XXX.XXX". During the analysis of the network traffic of the "TURKCELL_eFATURA.exe" TorrentLocker ransomware, it was determined that the malicious software attempted to communicate with the IP addresses "171.25.XXX.X" and "194.109.XXX.XXX".

To identify the domain or sources of the malicious software, WHOIS records were queried through the www.domaintools.com website (Figure 3). WHOIS records provide extensive information about the owners of internet domain names or IP addresses and related information.

This analysis enables the determination of the origins and domains of the ransomware, understanding who or what is behind the attack, and taking appropriate steps for mitigation. Such information gathering and analysis processes significantly contribute to cybersecurity professionals in detecting and defending against attacks and tracing the footprint of the attacker.



– Quick Stats

IP Location	Sweden Stockholm [redacted]
ASN	[redacted] Foreningen for digitala fri- och rattigheter, SE (registered Sep 28, 2011)
Resolve Host	maatusk[redacted]
Whois Server	whois.ripe.net
IP Address	171.25.[redacted]

```
% Abuse contact for '171.25.[redacted] - 171.25.193.[redacted] is ' abuse@dfri.net '

inetnum:        171.25.[redacted] - 171.25.193.[redacted]
netname:        SE-TORNET
country:        SE
org:            ORG-DFRI1-RIPE
admin-c:        ER6905-RIPE
admin-c:        EJ1830-RIPE
admin-c:        JN9999
tech-c:         JN9999
tech-c:         ER6905-RIPE
tech-c:         EJ1830-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         DFRI-MNT
mnt-routes:     DFRI-MNT
mnt-domains:    DFRI-MNT
notify:         noc@dfri.net
```

IP Information for 194.109.[redacted]

– Quick Stats

IP Location	Netherlands [redacted]
ASN	AS3265 [redacted]
Whois Server	whois.ripe.net
IP Address	194.109.[redacted]

```
% Abuse contact for '194.109.206[redacted]- 194.109.[redacted] is ' abuse@kpn.com '

inetnum:        194.109.[redacted] - 194.109.206.[redacted]
netname:        XS4ALL-CUST
descr:          XS4ALL Internet BV
country:        NL
admin-c:        XS42-RIPE
tech-c:         XS42-RIPE
status:         ASSIGNED PA
remarks:        Please send email to " abuse@kpn.com " for complaints
remarks:        regarding portscans, DoS attacks and spam.
mnt-by:         XS4ALL-MNT
created:        2006-10-24T17:35:00Z
last-modified:  2022-07-04T17:46:17Z
source:         RIPE
```

Figure 3. WHOIS records of the IP addresses contacted by the "TURKCELL_eFATURA.exe" file

4. Discussions

In this study, the "TURKCELL_eFATURA.exe" TorrentLocker ransomware has been extensively analyzed. The analyses provided an important step towards understanding the behavior of ransomware on computer systems and developing defense strategies.

As part of the analysis, file, directory, and registry movements of the "TURKCELL_eFATURA.exe" TorrentLocker ransomware, as well as network traffic analysis, were conducted. The results of these analyses allowed us to understand how the ransomware infiltrated the victim system, how it behaved on the victim system, and how it interacted. In particular, network traffic data recorded through Wireshark revealed that the ransomware attempted to communicate with specific IP addresses. By examining the WHOIS records of these IP addresses, potential information about the origins of the ransomware and the attackers was obtained.

Based on the analysis results, it is evident that the "TURKCELL_eFATURA.exe" TorrentLocker ransomware poses a serious cybersecurity threat. When such ransomware infiltrates computer systems, it can lead to significant data loss and financial damages.

On average, these types of ransomware demand approximately €1180 or $1500 per attack, significantly harming the economic impact [4]. Furthermore, ransomware serves as an effective tool for cybercriminals to achieve their objectives, possessing the capacity to propagate by targeting vulnerable systems. The prevalence of these attacks has been particularly high in countries such as Canada, Australia, and New Zealand, indicating a targeted dissemination pattern by the perpetrators.

5. Conclusion

In recent years, TorrentLocker has emerged as a significant threat within the cybersecurity realm, posing a serious risk to the digital data of users and organizations. This study conducts a real-case analysis to understand the strategies and techniques of TorrentLocker-type ransomware attacks. The analysis meticulously examines the attack strategy and how to trace and identify the post-attack trails left by the attacker.

The findings of this study aim to raise awareness among cybersecurity professionals, organizations, and individuals regarding TorrentLocker ransomware attacks, providing crucial insights into preventing such attacks and outlining the steps to be taken post-incident. The results play a critical role in developing defense strategies against future ransomware attacks and contribute significantly to the research in this field.

In conclusion, this work presents a comprehensive analysis of TorrentLocker ransomware attacks, offering guidance on cybersecurity measures to counteract these threats. Moreover, it is significant for developing new preventative measures and strategies within the context of combating this threat, providing a perspective necessary for the enhancement of cybersecurity defenses.

Article Information Form

Acknowledgments

The authors thank Comodo Group, Inc. USA for providing the malware dataset.

Funding

The research was supported by the Cankiri Karatekin University.

The Declaration of Conflict of Interest/ Common Interest

No conflict of interest or common interest has been declared by the authors.

The Declaration of Ethics Committee Approval

This study does not require ethics committee permission or any special permission.

The Declaration of Research and Publication Ethics

The authors of the paper declare that they comply with the scientific, ethical and quotation rules of SAUJS in all processes of the paper and that they do not make any falsification on the data collected. In addition, they declare that Sakarya University Journal of Science and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated in any academic publication environment other than Sakarya University Journal of Science.

Copyright Statement

References

[1] T. Meurs, E. Cartwright, A. Cartwright, M. Junger, A. Abhishta, "Deception in double extortion ransomware attacks: An analysis of profitability and credibility," Computers & Security, vol. 138, pp. 103670, 2024

[2] A. Mukhopadhyay, S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," International Journal of Information Management, vol. 74, pp. 102724. 2024.

[3] Malware Statistics, the AV-TEST Institute. [Online]. Available: https://www.av-test.org/en/statistics/malware/, 2024.

[4] Malware Statistics, the eset. [Online].https://www.eset.com/za/about/newsroom/press-releases-za/research/torrentlocker-cracked-europe-in-the-sight-of-bitcoin-requesting-ransomware1/, 2024.

[5] P. O'Kane, S. Sezer, D. Carlin, "Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis," Journal of Network and Computer Applications, vol. 7, no. 5, pp. 321-327, 2018.

[6] P. Sharma, S. Zawar, S. B. Patil, "Ransomware analysis: Internet of Things (Iot) security issues challenges and open problems inthe context of worldwide scenario of security of systems and malware attacks," In International conference on recent Innovation in Engineering and Management, vol. 2, no. 3, pp. 177-184. 2016.

[7] A. Alraizza, A. Algarni, "Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing," vol. 7, no. 3, pp.143. 2023.

[8] M. Cen, F. Jiang, X. Qin, Q. Jiang, R. Doss, "Ransomware early detection: A survey," Computer Networks, pp. 239, gmr.110138. 2024.

[9] K. Begovic, A. Al-Ali, Q. Malluhi, "Cryptographic ransomware encryption detection: Survey," Computers & Security, pp. 103349, 2023.

[10] T., Baker, A. Shortland, "The government behind insurance governance: Lessons for ransomware," Regulation & Governance, 2023, 17(4), pp. 1000-1020.

[11] A. Mukhopadhyay, S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach,"

International Journal of Information Management, pp. 74, gmr.102724, 2024.

[12] S. A. Syed, “Industry trends in computer software. In Ethical hacking techniques and countermeasures for cybercrime prevention,” pp. 54-59, 2021.

[13] I. Kara, M. Aydos, “The rise of ransomware: Forensic analysis for windows based ransomware attacks. Expert Systems with Applications,” pp.190, gmr.116198, 2022.