iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** II **Month of publication:** February 2025

DOI: https://doi.org/10.22214/ijraset.2025.38268

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

Malicious Ransomware Threats on Major Industry

M.C. Greenfield
Eastern Michigan University

Abstract: Malicious ransomware targeting large companies is the main topic of this paper. It describes the steps that organizations should take to stop these assaults. Ransomware attacks in the banking and finance sector, executed by groups like hacker groups, have become far more frequent.

I. INTRODUCTION

The FBI received over 799,000 cybercrime frustrations in 2019, with claimed damages reaching over 4 billion USD. Ransomware assaults may result in expensive operational interruptions as well as the reduction of vital facts. Ransomware represents a form of a pernicious application program (also known as malware) that prohibits users from gaining access to linked computers, organized frameworks, or file documents and requirements that one pays a shakedown to regain access to them. Ransomware can be mistakenly installed on a computer via accessing an electronic message or watching an advertisement. Accessing a webpage or browsing a malware-infected webpage can also install ransomware on a computer. The application program is installed on a system that prevents entrance to the computer and the file documents and information (FBI, 2021). Given that ransomware targets several organizations and is present in Russia, America, and Ireland, it may be harmful to the world.

II. MALICIOUS RANSOMWARE IN AMERICA

A series of destructive ransomware assaults has shaken America, such as the recent significant intrusion of a major software company and a suspected targeted intrusion on the council of Republicans. In light of developments, both the private sector and governmental agencies in America are trying to figure out how the national legislative body and specific firms should deal with the rising threats. A Miami-based computer application business reported in the seventh month of 2021 that it was probing a suspected cyber assault on its remote monitoring computer application, an IT management tool. According to the Miami-based computer application business, numerous clients utilize the hacked program to supply less involved IT services to over 900 thousand other firms (Jeffery & Ramachandran, 2021).

According to the Miami-based computer application business (Kaseya), the hack affected slightly over 1400 of those organizations, calling it among the most significant ransomware assaults to date. Hackers linked to the Ransomware criminal gang demanded over 69 million USD in digital currency ransom to release the hijacked data. No harm came to vital foundations in America due to the onslaught (Jeffery & Ramachandran, 2021).

As a result of the epidemic, cybercriminals targeted businesses that were impacted the worst, including municipal regions, academic institutions, and health services. These cybercriminals also see the global outbreak of attacking workers who are now staying home on their machines. A risk assessment involves a critical, objective analysis of an organization's entire protective system and its vulnerabilities. Ransomware criminals are increasingly targeting management suppliers, a framework that supports a lot of customers simultaneously. This aspect implies that if an attacker obtains entrance to one management supplier, they may also acquire access to the customers it serves. Some frequently hijacked management suppliers due to inadequately protected isolated entrance capabilities (Sobers, 2021).

III. MALICIOUS RANSOMWARE IN IRELAND AND RUSSIA

In research from Winder (2021), companies are suffering as a result of ransomware assaults. Information technology (IT) directors must learn something from several of the year's most significant cyberattacks. A study of over several thousand worldwide IT leaders verified what many had surmised. Many leaders believe that ransomware assaults are on the rampage. According to the risk assessment team participating, ransomware assaults increased by nine times as great between January 2020 and June 2020. This analysis is consistent with a report from cybersecurity officials of the island of Great Britain between January 2021 and June 2021. This report revealed that over 21 percent represented malware that encrypts systems. The following are five of the main assaults in 2021: CNA Financial, Brenntag, Ireland's Health Service Executive, Kaseya, and Colonial Pipeline.

Although CNA is one of the globe's top ten commercial insurance companies, in March 2021, it paid out a 40 million USD payoff 14 days after cybercriminals seized datum values and froze its computers, according to a data and media company. By the middle of the same month, the company commenced activities. Assumed to be a Russian-affiliated gang, the hackers deployed a fresh variant of a Phoenix malicious virus. This nasty virus scrambled data on over fifteen thousand high-performance computer systems on its business networking system (Kass, 2021). From March to June of 2019, cybercriminals delighted in hacking into computerized frameworks. Baltimore experienced a phishing encrypting malware assault in the same year, which rendered the area's technical, and informational systems inoperable. During the same period, a different ransomware assault struck twenty-three government organizations throughout the state of Texas. However, anyone can fall prey to ransomware regardless of status. As experts of accounting reports, leaders in accounting are the main ones that safeguard datum values (Moorcraft, 2021).

Severe genuine disturbances could occur whenever cybercriminals acquire entry into a corporate support system even though current attacks befall other types of companies. Chemical firms are still not invulnerable to cybercrime. Recent cyberattacks on major companies ceased production and some other activities as the companies probed the intrusions. Brenntag said it does not discuss any hacking-related complaints or requests. According to an email from the firm, it had minimal details concerning the safety problem in the northern continent and employed computer security experts to engage in the probe (Bomgardner, 2021). Brenntag's North American operation was the subject of a payoff malware assault. The taunt players encrypt hardware on the networking system and steal files not encrypted as elements of their assault. According to material provided by another company, the DarkSide ransomware gang professed to have taken over 148 GB of data throughout their invasion. The ransomware ring built a personal data breach web page explaining the sorts of data and images of some of the files to back up their professions (Abrams, 2021). See Figure 1.

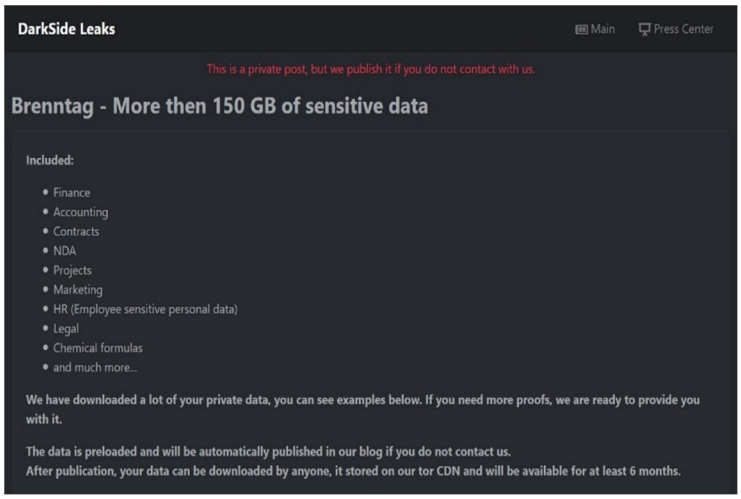


Figure 1 Private Data Leak

Note. Page Delivered to Brenntag (Abrams, 2021)

According to Bleeping Computer, Brenntag SE submitted a $4.4 million decentralized digital currency extortion to the DarkSide ransomware group. During May's second week, this payment took place to get a decoder for documents encoded by the cybercriminals throughout a ransomware assault on the firm (Business Insurance, 2021). The leading DarkSide group receives up to thirty percent of ransom money as a portion of this deal, with the balance going to the partner that carried out the assault. These ransomware deals often require that the accomplice reveal how they acquired entrance to the victim's computer. The DarkSide associate alleges to have gained access to the network after receiving stolen credentials in this instance. The DarkSide partner, on the other hand, has no clue how they acquired the authorizations in the first place (Abrams, 2021).

Worldwide guidelines and governmental groups are currently debating how to enhance and revise the responsibility structure and limit with regard to artificial intelligence and technological advances. However, given the intricacy of the issue and the disparate juridical systems worldwide regarding personal responsibility, it is unlikely that a unified and consistent reaction will be reached anytime soon. Furthermore, cyberattacks targeting vital infrastructure sectors, such as utilities may be detected and responded to with the help of machine intelligence. Likewise, proper management of cybersecurity solutions may help lower and reduce safety hazards (Velasco, 2022).

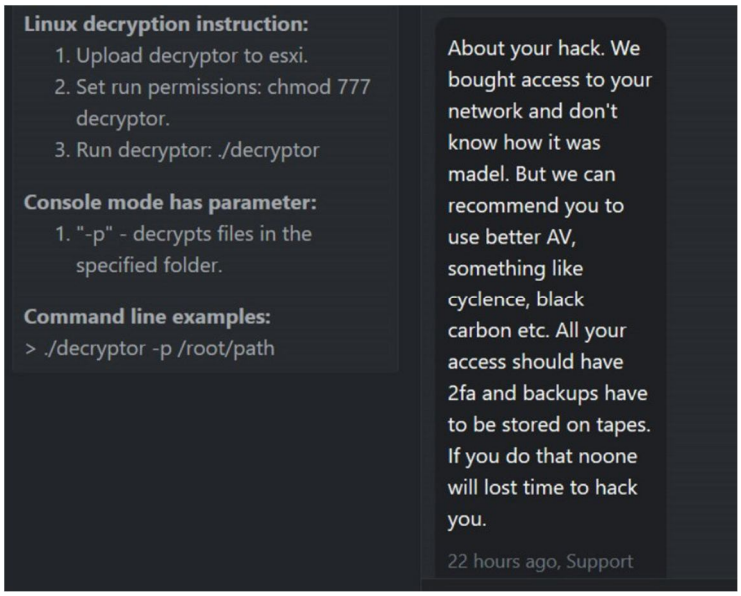
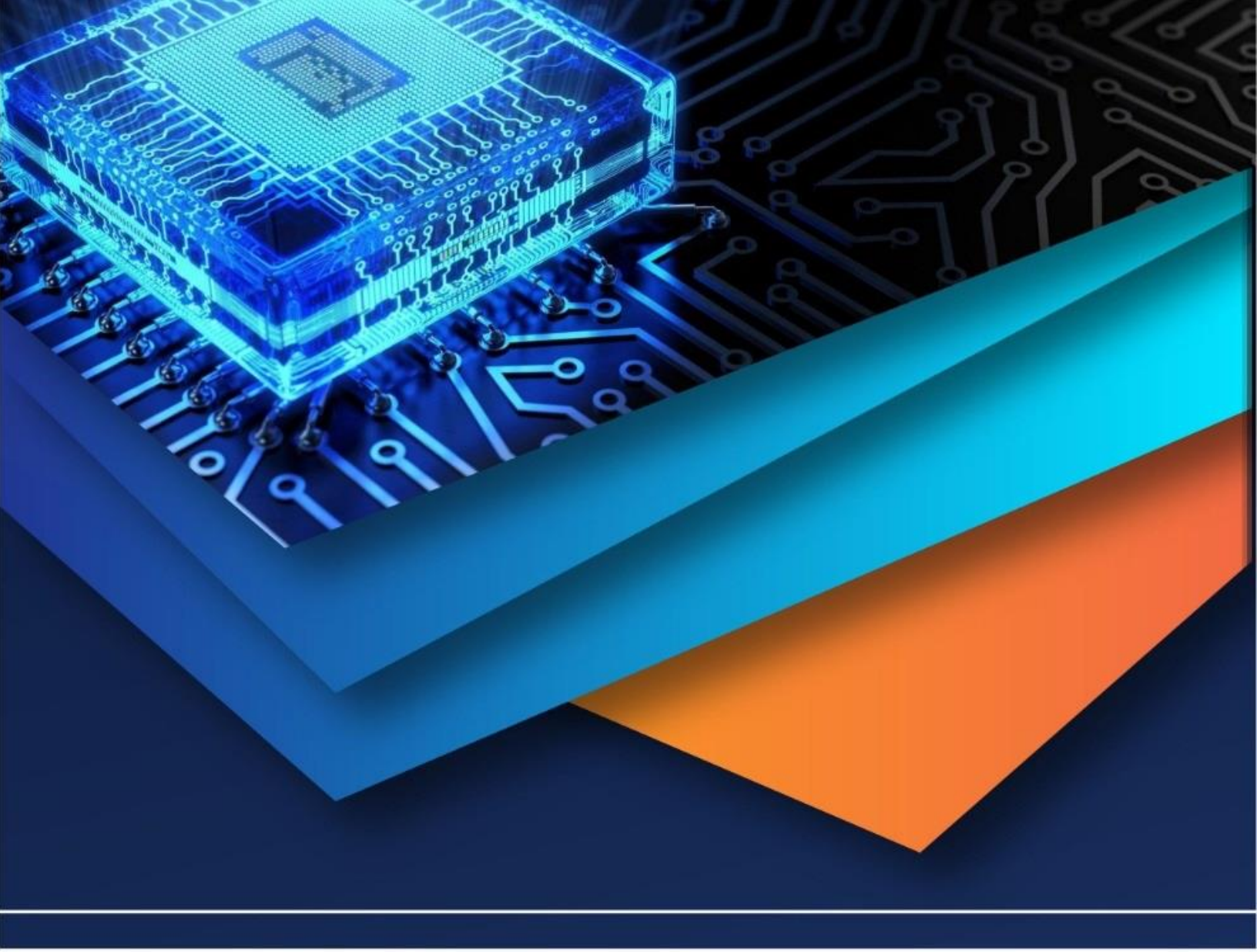


Figure 2 DarkSide
Note. Page Delivered to Brenntag (Abrams, 2021)

REFERENCES

[1] Abrams, L. (2021, May 14). Chemical distributor pays $4.4 million to DarkSide ransomware. BleepingComputer. https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/
[2] Bomgardner, M. B. M. (2021, May 27). Chemical firms hit by cyberattacks. Chemical & Engineering News. https://cen.acs.org/business/specialty-chemicals/Siegfried-Brenntag-Symrise-hit-cyberattacks/99/i20
[3] FBI. (2021, June 4). Ransomware. Federal Bureau of Investigation. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
[4] Jeffery, L., & Ramachandran, V. (2021, July 8). Why ransomware attacks are on the rise — and what can be done to stop them. PBS NewsHour. https://www.pbs.org/newshour/nation/why-
[5] ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them
[6] Kass, H. D. (2021, May 24). Insurer CNA Paid Hackers $40M for Ransomware Decryption. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/cna-payment-40-million-dollars/
[7] Kovacs, E. (2021). FBI: Cybercrime Victims Reported Losses of $4.2 Billion in 2020 | SecurityWeek.Com. SecurityWeek - A Wired Business Media Publication. https://www.securityweek.com/fbi-cybercrime-victims-reported-losses-42-billion-2020
[8] Moorcraft, B. (2021, July 14). CNA finalizes investigation into cyberattack. Insurance Business America. https://www.insurancebusinessmag.com/us/news/cyber/cna-finalizes-investigation-into-cyberattack-260687.aspx
[9] Sobers, R. (2021, July 7). 81 Ransomware Statistics, Data, Trends and Facts for 2021 | Varonis. Inside Out Security. https://www.varonis.com/blog /ransomware-statistics-2021/
[10] Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum, 23(1). https://doi.org/10.1007/s12027-022-00702-z
[11] Winder, D. (2021, September 22). The Five Most Important Ransomware Attacks of 2021. Raconteur. https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY