Page 2211 - 2217 **DOI:** *https://doij.org/10.10000/IJLMH.116358*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

© 2023 International Journal of Law Management & Humanities

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **Gyan@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

The Impending Impact of the Drinik Virus on Micro Small and Medium Enterprises

SOUMYA CHAKRABARTI[1], AMAN HASAN[2] AND HUMAM ZAFAR[3]

ABSTRACT

As India grapples with the Drink's virus and its impact on big financial institutions, little attention is given to the vulnerability of Micro, Small, and Medium Enterprises (MSMEs) to cyberattacks and the potential havoc that Drinik malware can wreak on this vital sector. This article sheds light on the significance of MSMEs in the Indian economy, their susceptibility to cyber threats, the consequences of cyberattacks, and the association between MSMEs and the Drinik virus. The research underscores the need for MSMEs to invest in robust cybersecurity technologies and empower their employees to counter cyber threats effectively. In developing countries like India, where internet privacy and cyberspace are critical concerns, understanding the impending impact of the Drinik malware on MSMEs becomes crucial. With MSMEs constituting a substantial portion of India's GDP and employment, safeguarding their operations from cyberattacks assumes paramount importance. Limited resources and outdated technologies further exacerbate their vulnerability. This article reveals the potential ramifications of cyberattacks on MSMEs, both in terms of financial losses and reputational damage. To mitigate these risks, MSMEs must prioritise investments in cybersecurity measures and foster a culture of cyber resilience among their workforce.

Keywords: *MSMES, Drinik virus, cybercrime.*

I. INTRODUCTION

In India, everyone is concerned about Drinik[4] virus impact in big financial institutions no one is concerned about its effect on Micro Small and Medium Enterprises hereinafter referred to as MSMEs and how much vulnerable MSMEs already are to cyberattacks if Drinik targets MSMEs then it will create a major impact not only in MSMEs but in the overall economic situation of India. Not only that, most of the cases related to cyberattacks on MSMEs remain unreported because they do not think that is necessary to report. Drinik virus, a type of malware that can

[1] Author is a student at Jamia Millia Islamia, India.
[2] Author is a student at Jamia Millia Islamia, India.
[3] Author is a student at Jamia Millia Islamia, India.
[4] Bill Toulas, Android malware now targets users of 18 Indian banks, Bleeping Computer® LLC (Oct 27, 2022, 01:10 PM), https://www.bleepingcomputer.com/news/security/drinik-android-malware-now-targets-users-of-18-indian-banks/.

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

steal personal information and bank credentials, poses a major threat to MSMEs as most of their business operations are conducted online. The document emphasizes that MSMEs should invest in effective cybersecurity technology and empower their employees to protect themselves against cyber threats. This research paper focuses on Internet privacy and cyberspace in third-world countries, focusing on the impending impact of the Drinik malware on MSMEs. This article discusses the importance of MSMEs in the Indian economy, why MSMEs are more vulnerable to cyberattacks, the impact of cyberattacks on MSMEs, and why MSMEs are associated with Drinik Virus. MSMEs contribute a significant portion of India's GDP and employment, making them important for the country's growth and development. However, due to limited resources and outdated technology, MSMEs are more vulnerable to cyber attacks than large companies. The data shows the potential impact of cyberattacks on MSMEs, finance, and reputation. The document emphasizes that MSMEs should invest in effective cybersecurity technology and empower their employees to protect themselves against cyber threats.

II. THE SIGNIFICANCE OF MSMES IN INDIA'S ECONOMY

1. MSMEs contribute to nearly 27% of our country's GDP. As per the official MSMEs annual report of 2022-23[5]The total number of MSMEs in India is 633.9 lakh out of which 324.9 lakh MSMEs (52.3%) are in rural areas & 309 lakh MSMEs (48.8%) are in urban areas.
2. With the above number of MSMEs, you can assume the number of employment it is generating. MSMEs employ around 120 million persons, becoming the largest employment-generating sector in India after agriculture.
3. MSMEs are also encouraging the export of domestic goods and services which is increasing the potential of Indian products in foreign markets.
4. MSMEs provide employment opportunities mostly to the weaker sections of society like women, workers, artisans, etc., and play a major role in developing their social entrepreneurship skills.
5. MSMEs create a wide variety of goods and services that promotes the government's "Make in India" scheme and also at the same time make India self-reliant.
6. MSMEs promote innovation by helping and supporting entrepreneurs who have creative goods and services providing ideas.

[5] MSME Annual Report 2022-23, MSME, Ministry of Micro, Small & Medium Enterprises, Government of India, (Mar 14, 2023, 10:00 AM), https://msme.gov.in/msme-annual-report-2022-23.

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

From the above points, you can see that if any difficulty arises in the growth of MSMEs then how drastically it can affect the growth and development of our nation?

III. Reasons why MSMEs are more vulnerable to cyberattacks

Since India is becoming a digital economy, most of its economic transactions are online. The Indian government is also taking various initiatives to promote the use of digital platforms. During the COVID-19 outbreak, there was a major shift in transactions in MSMEs from offline to online. The major problem of MSMEs is that they have a fixed amount of capital with them so they cannot change their technology frequently but that is not the case with big companies. They have large amounts of capital so they can change their technology according to the needs of society whenever they want. But the technology that MSMEs are using is mostly obsolete making them vulnerable to cyberattacks. Most of the workers engaged in MSMEs are not proficient in dealing with cyberattacks making them most vulnerable to cyberattacks. MSMEs do not have sufficient capital to invest in good cybersecurity technology and also they have simpler data-handling processes. Another reason is that MSMEs mostly neglect and don't consider investing in cybersecurity because they think that only big companies are the victims of cybercrimes. But they don't know that it is easier to attack MSMEs than big companies because they do not have complex cybersecurity measures to secure their data. Now, most of the work of MSMEs is done remotely and also it is very difficult for MSMEs to upskill their workers according to the new age world. It is also difficult for MSMEs to hire skilled and competent workers. MSMEs also lack technological innovation and business expertise.

IV. Implications of cyberattacks on MSMEs

Now first of all MSMEs do not have a large number of customers like big companies. So, if their customers' sensitive information got leaked then this will affect their reputation and goodwill in the market and it will cause them to lose their customers. If they lose their customers then they will face loss and it can eventually lead to the shutdown of their business. Cyberattacks create two major effects on MSMEs: the first one would be financial loss and the other one would be reputation loss. But these two are not the only problems that MSMEs would face from cyberattacks. Another problem would be that they might not be able to compete with foreign companies that have advanced cybersecurity technologies.

V. What makes MSMEs particularly susceptible to the impact of the Drinik virus?

In India everyone is concerned about Drink's impact on big financial institutions no one is

concerned about its effect on MSMEs and how much vulnerable MSMEs already are to cyberattacks if Drinik targets MSMEs then it will create a major impact not only in MSMEs but in the overall economic situation of India. Not only that, most of the cases related to cyberattacks on MSMEs remain unreported because they do not think that is necessary to report.

If we look at the background of Drinik then we will know the potential of this virus to change itself and its abilities. It came in 2016 at that time Drinik malware was only able to steal data with the help of phishing. But in 2022 Drinik changed itself from being malware to an Android Trojan and now it can overlay assaults, keylogging, screen recording, etc to steal the personal information and banking credentials of potential taxpayers[6]. It targeted customers of 18 big Indian financial institutions by creating an application called iAssist. Once installed this application uses accessibility services to gain control over the phone and when you try to claim the income tax refund it screen records your banking credentials like credit card, debit card numbers, and also other personal information. It is very difficult to identify this virus in your phone. Now, the main question is how this virus can affect MSMEs. So, you know that nowadays after COVID-19 most MSMEs are doing their economic transactions in online mode where their customers pay them on their websites or in their apps. So, when their customers try to pay them this virus can steal their banking credentials and personal information like their account number, CVV, pin code, etc. Now, this virus can also use the personal information of their customers to sell them on the Black web. MSMEs mostly ignore this fact; they might be on the next list of attacks after big financial institutions. There are a few cases where Small Businesses get affected because of cyber attacks.

The first case would be Escrow[7], a California-based company that was attacked by a "Trojan Horse" malware that steals $1.5 million from their bank account which leads to the shutdown of their business. Look at the potential of this Trojan virus. At first, it acquired the company's bank data and then misappropriated it. Just like this virus, Drinik is also a Trojan which can do much more harm to MSMEs than it has done to banks.

There was another case where a small business was affected by cyberattacks. It was a case of Green Ford's Sales company which was a car dealership company in Kansas. This company lost $23,000 when hackers stole their banking information and they made 9 fake employee accounts and paid them. The company was not able to catch them initially. Additionally, in this case, we

[6] Sneha Kulkarni, Drinik: How this malware targets income tax payers, The Economics Times, (Nov 10, 2022, 03:38 PM), https://m.economictimes.com/wealth/save/drinik-how-this-malware-targets-income-tax-payers/articleshow/95317681.cms.

[7] Stories from Small Businesses that were Attacked, Syscon, (June 16, 2023, 9:10 PM), https://syscon-inc.com/stories-from-small-businesses-that-were-attacked/.

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

can see that the method this hacker used to steal money was different from other cases. Let's focus on a different case of Wright Hotels which is a real estate development firm that was attacked by a virus that stole the email of the company and then impersonated the owner of the company and then drained $1 million from the company's bank account. Now, take another example of a Maine-based PATCO Construction Company which lost $588,000 in a Trojan Horse cyber heist. But the company was able to get a small amount of money back.

The cases mentioned above show us how vulnerable small businesses are to cyberattacks. These cases are not of India but of developed nations where they ensure good cybersecurity measures still they get targeted by Trojan. But Indian MSMEs are even more vulnerable ffromDrinik. And the fact that is concerning is that the developers of Drinik are always trying to make Drinik even more and more advanced. Back in 2016, it was only able to steal SMS but now it can do much more than that. In a few years, Drinik was able to become even more dangerous than it was before.

VI. ASSESSING THE ADEQUACY OF CURRENT CYBERCRIME LAWS FOR MSMES

CERT-In: Computer Emergency Response Team has been created under Section 70B[8] of the Information Technology 2000 to deal with instant cyberattack incidents. If any company faces any problem related to cybercrime they can immediately report it to this agency and this agency will try to investigate it with the available resources it has. But the problem is that most of the cases of cybercrimes against MSMEs remain unreported because people don't consider it important to report the cyberattack. After all, it is really rare to recover the money drained from a cyberattack.

Cyber Cells: In every state of India there are a large number of Cyber cells formed by the government. So, people aggrieved by cyberattacks can report and lodge an FIR against the hackers. But the problem is that it is very difficult to find the exact location of the hacker and in most of the cases, it shows that the hacker is not from India. And also if cyber cells can confirm a particular location of the hacker. It is difficult to find that particular person who hacked. The chances of finding one are very low. For example- If the cyber cell can track the location of the hacker who is present in Russia. But even if you can know their location it is difficult to know the identity of any particular individual or group involved in that cybercrime.

Adjudicating Authority under the IT Act: A complaint can also be filed under Section 46[9] of the IT Act, 2000 to the adjudicating authority. But the problem is that the chances of getting the

[8] Information Technology Act, 2000, § 70B (India).
[9] Information Technology Act, 2000, § 46 (India).

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

cyberattack problem resolved are very low. And it is also uncertain if you will be able to find the hacker or not and also it is very difficult to find his location.

Civil Suit: A person who has suffered from cyberattacks can initiate civil proceedings against that person. But what would happen if we don't know the identity of the hacker against whom are you going to initiate those proceedings? This is the main question that remains unanswered.

Section-66[10] of IT Act, 2000- "*Computer-related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both*." This section of IT Act 2000 deals with the punishment but it can only become effective if we know about the identity of the developers of DDrinikwithout their identity how can the court charge them with punishment?

Section-66C[11] Of IT Act, 2000- "*Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh*." This act is also used to punish someone who steals someone's personal information and banking credentials with the help of a computer or any electronic gadget and then uses that to drain money. Also in the case of Drinik it tries to steal the personal data of the customers of big financial institutions with the help of a fake website. Even though you have this section to punish hackers, we do not have any laws to regulate this malware, trojan, etc. in the first place before it can attack anyone.

Section-66D[12] of IT Act, 2000- "*Punishment for cheating by personation by using computer resources.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees*." This act gives punishment if anyone steals personal information with the help of a computer and uses it to impersonate that person to gain unfair benefits. The main fact that makes this law ineffective is that it is very difficult to know that imposter's identity and without that person's identity how can we punish him?

[10]Information Technology Act, 2000, § 66 (India).
[11]Information Technology Act, 2000, § 66C(India).
[12] Information Technology Act, 2000, § 66D (India).

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

VII. Recommendations

1. First of all, the government should provide cyberattack insurance to all MSMEs so that they can at least recover from their loss. The major loss from a cyberattack is faced by MSMEs because not only do they suffer financial loss but they also suffer reputation loss which affects their whole business but there is no such insurance policy particularly to cover the damages suffered from cyberattacks by MSMEs by the government.
2. The Central government should direct the state government to organize cyberattacks awareness campaigns and workshops to inform them about Drinik, particularly for all the MSMEs of their respective States. This initiative will help MSMEs to become aware of the situation and how to deal with that situation. Government should organize this type of campaign once every month.
3. Government should also ban the functioning of sites like the Black Web where the stolen data is sold illegally. In India, there is no law to regulate the functioning of such sites.
4. MSMEs should direct everyone who possesses the devices to not open any unauthorised emails.MSMEs should upskill their workers in cybersecurity and how to identify any potential cyberattack of virus-like Drinik.
5. MSMEs should regularly keep a check on the electronic devices and their condition and change all the outdated devices or software which they don't need anymore, especially those devices which are linked to their bank accounts.

VIII. Conclusion

MSMEs in general (micro, small and medium enterprises) are an important part of the Indian economy, accounting for around 27% of GDP and employing around 120 million people, mainly women workers. They also support the government's "Make in India" initiative to foster innovation and entrepreneurship and promote the export of local goods and services. However, as India moves towards a digital economy, MSMEs are more vulnerable to cyber attacks due to limited resources, backward technology, and security measures, inadequate cybersecurity, and insufficient investment in cybersecurity technology. Cyber-attacks can cause SMEs financial distress, reputational damage, and inability to compete with foreign companies. The Drinik virus is unique to MSMEs because of its ability to steal taxpayers' identities and credentials, which can affect their customers and lead to job losses. Therefore, MSMEs should be aware of the potential risks and invest in good cybersecurity tools to protect themselves and their clients from cyberattacks.

*****

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]