UDC 004.056
DOI 10.52171/herald.249

Analysis of Robocall Attacks, Methods of Protection Against this Threat

T.Sh. Alekberova, R.M. Haciyev

Azerbaijan Technological University (Ganja, Azerbaijan)

For correspondence:
Alekberova Tamara / e-mail: tamara.alekberova@gmail.com

Abstract

Cybercrime is recognized as any crime related to computers and the internet. It involves attacks on information about individuals, companies, or governments. When individuals are the primary target, their computers are used as tools in cybercrime. Cybercrimes also include traditional crimes committed with internet access. For example, telemarketing, internet fraud, identity theft, and credit card fraud are current examples of cybercrimes. In other words, cybercrime can be classified as an act of violence carried out using any device with internet access. Billions of robocalls are made around the world every month. Thanks to technology, telemarketers and scammers can make robocalls over the internet. Some robocalls may offer useful information, such as appointment reminders or canceled flights. However, they primarily aim to sell you something, and many of them are scams. When these calls are made, the caller often hides behind various excuses. The article analyzes the current cyber threat and analyzes ways to protect against this attack.

Keywords: internet, virtual networks, cyberattack, cybercrime, robocall.

Submitted *13 Jan 2025*
Published *17 Mar 2025*

For citation:
T.Sh. Alekberova
[Analysis of Robocall Attacks, Methods of Protection Against this Threat]
Herald of the Azerbaijan Engineering Academy, 2025, vol. 17 (1), pp. 99-104

Robocall hücumlarının təhlili, bu təhlükədən qorunma metodları

T.Ş. Ələkbərova, R.M. Hacıyev
Azərbaycan Texnologiya Universiteti (Gəncə, Azərbaycan)

Xülasə

Kibercinayətlər kompüter və internetlə bağlı hər hansı cinayət kimi tanınır. Bu, fərdlər, şirkətlər və ya hökumətlər haqqında məlumatlara hücumları əhatə edir. Fərdlər əsas hədəf olduqda, onların kompüterləri kibercinayətkarlıqda alət kimi istifadə olunur. Kibercinayətlərə internetə çıxışla törədilən ənənəvi cinayətlər də daxildir. Məsələn, telemarketinq, internet fırıldaqçılığı, şəxsiyyət oğurluğu və kredit kartı fırıldaqları kibercinayətlərin cari nümunələridir. Başqa sözlə, kibercinayət internetə çıxışı olan istənilən cihazdan istifadə etməklə həyata keçirilən zorakılıq aktı kimi təsnif edilə bilər. Dünyada hər ay milyardlarla robot zəng edilir. Texnologiya sayəsində telemarketlər və fırıldaqçılar internet üzərindən robot zənglər edə bilərlər. Bəzi robot zənglər görüş xatırlatmaları və ya ləğv edilmiş uçuşlar kimi faydalı məlumatlar təklif edə bilər. Bununla belə, onlar ilk növbədə sizə bir şey satmağı hədəfləyirlər və onların çoxu fırıldaqlardır. Bu zənglər edilən zaman zəng edən şəxs çox vaxt müxtəlif bəhanələr arxasında gizlənir.Məqalədə mövcud kibertəhlükə təhlil edilmiş və bu hücumdan qorunma yolları analiz edilmişdir.

Açar sözlər: internet, virtual şəbəkələr, kiberhücum, kibercinayət, robot zəng.

Анализ атак роботов-вызовов методы защиты от этой угрозы

Т.Ш. Алекберова, Р.М. Гаджиев
Азербайджанский технологический университет (Гянджа, Азербайджан)

Аннотация

Киберпреступностью признается любое преступление, связанное с компьютерами и Интернетом. Это включает в себя атаки на информацию об отдельных лицах, компаниях или правительствах. Когда основной целью являются отдельные лица, их компьютеры используются в качестве инструментов киберпреступности. Киберпреступления также включают традиционные преступления, совершаемые с доступом в Интернет. Например, современными примерами киберпреступлений являются телемаркетинг, интернет-мошенничество, кража личных данных и мошенничество с кредитными картами. Другими словами, киберпреступность можно классифицировать как акт насилия, совершаемый с использованием любого устройства с доступом в Интернет. Каждый месяц по всему миру совершаются миллиарды звонков от роботов. Благодаря технологиям телемаркетеры и мошенники могут совершать звонки через Интернет. Некоторые вызовы роботов могут содержать полезную информацию, например напоминания о встречах или отмене рейсов. Однако в первую очередь они стремятся вам что-то продать, и многие из них являются мошенничеством. Когда совершаются такие звонки, звонящий часто прикрывается различными оправданиями. В статье анализируется современная киберугроза и анализируются способы защиты от данной атаки.

Ключевые слова: интернет, виртуальные сети, кибератака, киберпреступность, робот-вызов.

Introduction

Developments in information and communication technology have provided advantages such as communication, quick access to information, and global trade. Additionally, both individuals and institutions face new economic lifestyles and opportunities, which come with certain challenges. Information, particularly internet technologies, has become essential in every field, especially in business, where they are increasingly used to remain competitive, ensure sustainability, and facilitate easy access to new economic advantages [1]. Instant access to products and services over the internet has enhanced the functionality and efficiency of organizations across all sectors, including production and inventory control, as well as supply chain management, especially in trade.

However, alongside these positive impacts, the use of the internet and information technologies also brings cyber threats and attacks aimed at accessing databases where production and stored data reside. The types and applications of these attacks are constantly evolving, and they are expected to manifest more destructively in the near future.

Nevertheless, businesses have limited information about the potential damage they may face and often lack adequate protection against cyber threats and attacks. Information systems have created significant environments and opportunities for terrorist organizations and cybercriminals to engage in illegal activities, leading to new avenues for illicit revenue [2].

Attacks on government agencies, private organizations, and individual information systems pose a threat to our country, as they do worldwide. Attacks from hackers and cyberterrorist organizations can harm many sectors and significantly damage the national economy. Despite the fact that cyberattacks and threats are dangers for all sectors, a lack of awareness about cyberattacks and the failure to implement necessary precautionary measures highlight the seriousness of this threat [3].

Robocall Attack. A robocall refers to calls made automatically by a computer system that share pre-recorded messages. In the past, robocalls were primarily associated with telemarketing, political messages, and surveys conducted by election candidates. However, they have become particularly notorious in the U.S. for capturing individuals' personal information through phone conversations and using it for malicious purposes [4]. Automatic bot calls are also referred to as spam calls or fake calls.

While there may be beneficial uses for automatic calls, such as informing a company's users or school parents, or notifying the public in emergencies, fake spam calls receive backlash in many different parts of the world due to their fraudulent nature.

This system is becoming increasingly prevalent because searches can be easily conducted using software that even someone with limited technical knowledge can operate, thanks to low costs associated with searching. The virtually zero barriers to entry mean that anyone with malicious intent can easily utilize this system.

What makes fake calls particularly dangerous is the ability of relevant software to display the calls as coming from completely different numbers. VoIP (Voice over IP) technology allows users to change their number from anywhere in the world, making it seem as if they are calling from the desired country [5].

For example, a scammer on the other side of the world can manipulate the system to make it appear as though they are calling from your bank in your country. This can lead to people answering calls they would typically ignore, putting them at greater risk of falling victim to scams.

Key Features of Robocall Attacks.

Robocall attacks involve mass calling campaigns conducted through automated phone calls. These calls are typically used for various purposes, such as advertising, fraud, political campaigns, and more. Many robocall attacks are illegal or unwanted, causing significant distress for users.

We can divide the key features of robocall attacks into 8 parts.

1. Automated Calls

Robocalls are executed with the help of automated systems. These systems can make thousands of calls quickly through computers programmed with specific algorithms or automatic calling applications installed on phones. These calls are carried out using pre-recorded messages, which typically include sales offers, surveys, advertisements, political messages, and more.

2. Fake Numbers

Robocalls often use "caller ID spoofing" technology to execute attacks. This technology displays a fake number as the one receiving the call. By doing this, the caller hides their real number and shows familiar or local numbers to convince users to answer the call. This increases the likelihood that users will pick up the call and trust the incoming number.

3. Fraud

Statistics indicate that the majority of robocalls are intended for fraudulent purposes. These calls often present users with various scam schemes, the most common of which include:

- Notifications about fake lotteries or prizes.
- Phishing attack calls aimed at stealing bank or financial information.
- Fake notices related to tax debts or legal issues.
- Offers of counterfeit products or services.
- Scammers pressure users to take immediate action, such as demanding payment quickly because an offer is about to expire or requesting credit card information under the pretext of protecting personal data.

4. Advertising

While some robocalls may be legal, advertising calls made without users' consent are considered illegal. These calls promote products or services. When users opt out of such calls, the calling company is required to honor that request, but this rule is not always followed. Despite numerous complaints, these calls may continue. Sometimes, incoming calls appear to come from a legitimate company number but are actually made by a scammer.

5. Political Campaigns

During election periods, political parties or candidates use robocalls to disseminate their messages and engage with voters. These calls provide detailed information about the candidates, solicit support for campaigns, and share information about election dates and polling locations. While these calls may be legal in some instances, they are often unwanted and can cause annoyance.

6. Surveys and Polls

Some robocalls ask users to participate in surveys and polls. During these calls, users are

asked questions on various topics and their opinions on those questions are solicited. These calls are often used to gather information for commercial purposes.

7. Security and Privacy Risks

Phishing: Robocall attacks often present users with various fraudulent scenarios to steal their personal information (e.g., social media accounts, bank details, credit card numbers, etc.). Scammers frequently impersonate representatives of banks, government organizations, or well-known companies.

Vishing (Voice Phishing): This type of attack is a form of phishing conducted through voice calls. Users are asked to provide confidential information (e.g., the CVV number of a bank card), which is then used for fraudulent purposes.

8. Legal and Regulatory Measures

Various countries have laws and regulatory measures in place to combat robocall attacks, and these are continually developed to meet demand. For example, in the United States, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) implement various rules and penalties to address robocalls. Other countries have enacted similar laws. In Azerbaijan, the existing laws include the following.

Robocall attacks remain a significant issue in today's world, and addressing this problem requires collaborative efforts from both users and legislative bodies. Strengthening this fight is possible through technological solutions, legal measures, and public awareness campaigns.

Methods for Protecting Against Robocall Attacks. As the name suggests, a robocall comes from a computerized automated caller, functioning like a robot. These calls often offer pre-recorded messages to promote political campaigns, telemarketing, or public service announcements.

Telemarketing calls, also known as internal sales, come from vendors or services encouraging consumers to purchase their products, while spam calls are a general term for unwanted calls that originate from suspicious numbers [6].

Robocalls designed to deceive people are illegal worldwide. In January 2020, the U.S. Congress passed the TRACED Act, which expands the Federal Trade Commission's mandate to combat spam calls with bipartisan support. This law increases penalties for robocalls from $1,500 to up to $10,000 per spam call.

According to an industry report by Truecaller, fraud attempts and financial scams are the most common reasons behind the majority of these calls. Spam calls lead to one in ten Americans losing money to phone scams..

According to data from the call protection company "First Orion," half of the calls received in 2019 were spam or automated calls. This highlights the need for more effective methods to block automated calls.

Conclusion

The identification and classification of various types of cybercrimes is an interesting topic for researchers for several reasons. One of the primary reasons is to provide a general definition of the concept of cybercrime [7]. Secondly, having a precise definition of what cybercrime results in helps researchers and practitioners determine the scope of the problem to be addressed. Thirdly, understanding the various aspects of cybercrime (such as distinguishing between the "technical" and

"human" dimensions of cybercrime) can assist law enforcement and criminal justice agencies in investigating, combating, and preventing such crimes.

Finally, identifying and differentiating various types of cybercrime allows researchers and practitioners to anticipate future trends in cybercriminality and develop timely solutions.

Conflict of Interests

The author declares there is no conflict of interests related to the publication of this article.

REFERENCES

1. H.Tu, A. Doupé, Z. Zhao, and **G.J. Ahn.** "Systems and methods for authenticating caller identity and call request header information for outbound telephony communications" (03.2016).

2. Guiora, A.N. What is Cybersecurity. Cybersecurity Geopolitics, law, and policy. Routledge, Newyork, 16-20. https://books.google.com.tr/.(27.01.2021).

3. Ələkbərova T.Ş. Blokçeyn texnologiyasında mövcud olan kiber hücumlar və Blokçeyn texnologiyasının təhlükəsizliyi. Azərbaycan Mühəndislik Akademiyasının Xəbərləri, 2024 cild 16, №3, s. 87-93.

4. CBS Netherlands. Less traditional crime, more cybercrime (2020).

5. Standler, B.R. Computer crime.http://www.rbs2.com/ccrime.htm (01.11.2020).

6. Grabosky P., Smith R. Telecommunication fraud in the digital age: The convergence of technologies. In Crime and the Internet, edited by David S Wall, London: Routledge. (2001), pp. 29-43.

7. Khan S.F., Portmann M., and **Bergmann N.W.** "A Review of Methods for Preventing Spam in IP Telephony," Modern Applied Science, vol. 7, no. 7, pp. 48, 2013.