Security Implications of Computer Botnets

Sándor Gyányi

Óbuda University, Kandó Kálmán Faculty of Electrical Engineering, Tavaszmező u. 15-17, 1084 Budapest, Hungary, gyanyi.sandor@kvk.uni-obuda.hu

Abstract: With the explosive growth in popularity of computer networks, so-called botnets appeared. These contain many infected smart devices that the owner can control remotely. The members of the botnet can carry out – usually illegal – tasks in a coordinated manner, which can cause significant damage to the targeted infrastructure. In addition to spam campaigns, Distributed Denial of Service attacks and other usual procedures, actions aimed at influencing public opinion are becoming increasingly popular, which can cause damage beyond IT environments. Popular social platforms have become targets for propaganda and other social engineering campaigns executed with the help of botnets. Another threat will be the growing use of artificial intelligence by attackers, which can significantly increase the effectiveness of the offensive activity of a botnet. In this article, I have tried to provide a comprehensive overview of the current and near-future risks to society posed by botnets and increasingly widespread artificial intelligence.

Keywords: malware; botnet; AI; LLM; DDoS; attacks; IT security

1 Introduction

With the help of computer networks, not only the classic, “traditional” computers can communicate with each other. By moving to the digital world, various electronic devices have “intelligent” control, so today, many smart technologies use such networks for communication purposes. Connecting devices with different capabilities and rather heterogeneous technological backgrounds also carries serious risks. Many modern devices contain a – sometimes unnecessary – computer inside. Every computer application, program or function library can contain errors, a natural part of complex IT systems. However, the interconnection of devices sometimes allows such programming flaws to be exploited remotely over a network. If the error is so serious that the attackers can install a malicious program code on the target device, they can gain control. This means they can download and execute applications to reach their desired goal. The popular name for such malicious program code installed on a victim computer is “malware”, a combination of “malicious software”.

These malicious programs run on the attacked device and thus have access to its entire set of resources (e.g. processor, memory, storage, network data transfer capacity). Since they can communicate with each other via computer networks – Local Area Networks or the global internet – it is, therefore, possible to make a distributed system out of them, that is, to make them take coordinated action with the help of central control. Such "hacked" devices are called zombies, robots, or bots for short; the network formed from them is usually called "botnet". The most important elements of botnets are:

- C2 (command & control) server. However, there are peer-to-peer solutions where any botnet member can act as a server.
- "Herder" which is the controller of the botnet, who assigns tasks to members. Also, known as "botmaster".
- Members who form the botnet. Usually, infected computers or other smart devices.

This article is based on personal experiences and extensive research using information from industrial sources.

1.1 Usages of Botnets

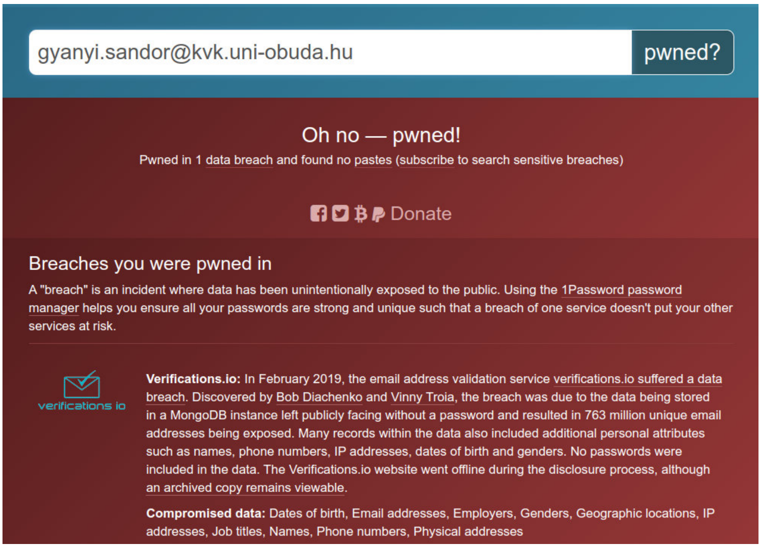
The size of botnets can vary greatly, depending on how successful the malware's infection activity was. Most malware tries to replicate itself, but the malware detection systems can identify and destroy the threat and the established botnet after some time. The strength of a botnet mainly lies in its size: the more devices it contains, the greater its computing capacity and the greater the network data traffic it can generate. Due to its distributed nature, a botnet can be used for tasks that can be effectively parallelized and divided into independent subtasks. This means the botnet members can be assigned to a partial task, which they can perform independently, and the result can be forwarded to a specific location. Some of the more popular application areas:

1.1.1 Password Cracking

Nowadays, the so-called "cloud" services have become significant. Most of these systems use authentication, some form of user registration. The popular method uses username-password pairs to identify and authenticate users, creating large databases of registered users' data. Such databases, which contain at least email addresses and passwords, are popular targets for attackers. If the protection of a web system is inadequate, stored user data can be leaked, usually in some form of database format. Fortunately, systems where the passwords are stored in an unencrypted – plain text – format is now rare. Usually, one-way encryption is used, and no simple method is available for decrypting these stored passwords. In doing so, the password provided by the user during registration is processed by a so-called “hash algorithm”, which produces a certain number of bits – usually a fixed length of data. The algorithm is specifically designed to scramble original bits that the original data cannot be restored by using purely the result. During the hash process, specific actions are performed that cannot be reversed because bit losses and overwrites occur. When logging in, the same password entered by the user is run through the same algorithm, so the same result should be obtained. If the generated bit sequence differs from the value created during registration, the wrong password has been entered, so the user's authenticity cannot be established. Decrypting passwords stored with this method – as the algorithm cannot be reversed – cannot be solved algorithmically. Brute force probing is the only possible solution. During this, different passwords must be generated – randomly or based on a dictionary – and run through the same algorithm used by the target system, and then check whether the obtained result can be found in the stored list. The correct password – or an equivalent sequence of characters – is found if so. Otherwise, the attempt must be continued.

This task can be perfectly parallelized; the list of possible passwords can be distributed among the botnet members so that the password cracking time can be drastically reduced.

These decrypted passwords can be used for hijacking accounts in different web applications, as, unfortunately, many people use the same password on different sites. On the black market, many password lists are available gathered from different data breaches.



gyanyi.sandor@kvk.uni-obuda.hu

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

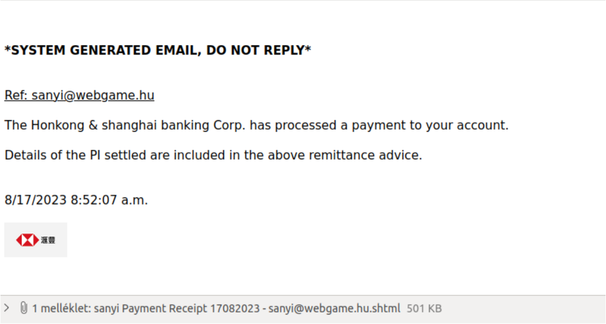
Figure 1

Data breach check on https://haveibeenpwned.com/

1.1.2 Spam Email Sending

Everyone who uses email has come across unsolicited mail. The type of these messages can be different:

- Marketing offers. The subject of these messages can be very diverse. They typically advertise products that cannot be advertised through traditional marketing channels (like medications, fake products).
- Malware. Some malware tries to infect others by sending emails to email addresses found in the address book of victim computer.
- Phishing. They try to take advantage of the credulity of users, usually impersonating an existing, authentic service provider. They try to direct the target person to the attacker's website and obtain their login or personal data.



SYSTEM GENERATED EMAIL, DO NOT REPLY

Ref: sanyi@webgame.hu

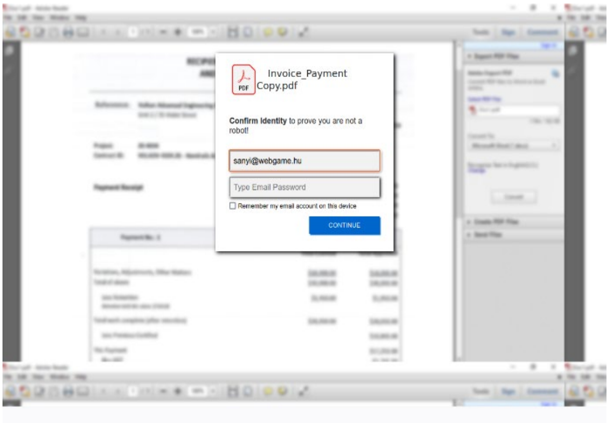
The Honkong & shanghai banking Corp. has processed a payment to your account.

Details of the PI settled are included in the above remittance advice.

8/17/2023 8:52:07 a.m.

1 melléklet: sanyi Payment Receipt 17082023 - sanyi@webgame.hu.shtml 501 KB

Figure 2
Phishing email



Invoice_Payment Copy.pdf

Confirm Identity to prove you are not a robot!

sanyi@webgame.hu

Type Email Password

□ Remember my email account on this device

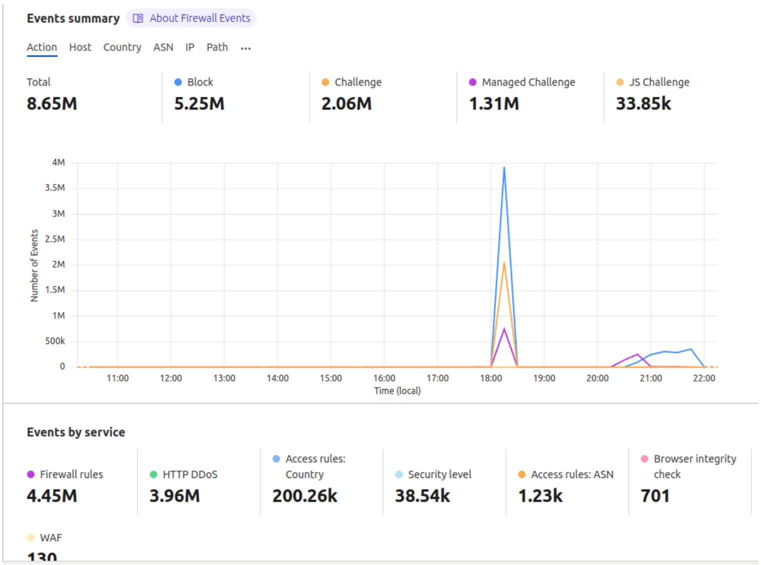
Figure 3
Phishing form

1.1.3 DoS and DDoS Attacks

In the classic data security threat triad – violation of Confidentiality, Integrity and Availability – the forced limitation of availability is a serious threat. Limiting availability is most easily achieved by causing overload in the targeted system. If the target is forced to perform too many tasks, the execution time can increase so much that it appears inoperable to users. Too many tasks mean the target lacks the resources to complete these requests in time. This way, an outage can be caused even if the target system is unknown to the attacker. Such attacks can be performed in several ways:

- By exploiting a known or newly discovered vulnerability of the target.
- By vastly overloading the communication channel used by the target, for example, by sending large amounts of unwanted data.
- By sending requests that make the target perform excessive tasks.

The usual name of these attacks is Denial of Service (DoS) or Distributed Denial of Service (DDoS) when the attacker uses a large number of hosts. A significant advantage of botnets is the ability to carry out DDoS attacks. Since they contain a large number of infected machines, the resources of these bots are adding up. It is very difficult to defend against them, as there is no well-defined profile for implementing defense. They are geographically dispersed, and many different networks could be involved, so network filtering based on the source address is impossible.



Events summary

Total	● Block	● Challenge	● Managed Challenge	● JS Challenge
8.65M	5.25M	2.06M	1.31M	33.85k

Events by service

● Firewall rules	● HTTP DDoS	● Access rules: Country	● Security level	● Access rules: ASN	● Browser integrity check
4.45M	3.96M	200.26k	38.54k	1.23k	701

● WAF
130

Figure 4

A DDoS attack timeline

As Figure 4 shows, the attacker caused an irrationally high request number in a very narrow time period. Most systems are scaled to the average, expected traffic. Depending on their size, botnets can carry out very large, so-called volumetric attacks, which often exceed the resources available to the average target. On February 11 and 12, 2023 – the weekend of the American Super Bowl – Cloudflare, a service provider specializing in protecting against DDoS attacks, prevented a record-breaking attack. The attacker botnet generated 71 million requests per second. [1]

1.1.4 Crypto Mining

The basic principle of cryptocurrencies is that they do not contain a central registry, but the authenticity checking is performed by endpoints operating in the system. During the verification of authenticity, it is necessary to make many mathematical operations, which require serious computing resources – primarily provided by the computer's central processing unit (CPU) or the Graphics Processing Unit (GPU) located on the video card. The computation also needs significant electrical power consumption, which could cost a lot of money for the device’s owner. If a botnet – more precisely, members of the botnet – perform the crypto-mining tasks, then the necessary computing power becomes “free” to the owner of the botnet, and unsuspecting owners of the devices will pay the price. To put this issue into perspective, the "Clipminer" botnet owners earned at least $1.7 million from crypto mining. [2]

1.1.5 Influencing Social Media

The use of social media has become extremely popular; more and more people use it to get information from there, but it can cause serious problems. There are specific processes and legal regulations to ensure the credibility of traditional media – newspapers, television, radio or news websites. Still, in the case of social media, these regulations and processes work with very limited efficiency. The primary goal of these social platforms is not to check the authenticity of the information published by its users but to increase the activity (engagement), as this can maximize revenues. The more committed and active a user is, the more pageviews and more additional content – like comments and “likes” – will be generated, which can push other users to engage. The more user activity, the more ads can be displayed to them. Thus, more advertisement revenue goes to the platform.

A proven – although not too ethical – method for increasing user activity is determining interests of the user as thoroughly as possible and to display corresponding content fit for these. Some would say this behavior is plain espionage, but the platform terms of service clearly describe and clarify these data usage conditions. How could the platform identify what users are interested in it? The most widely used process for content selection is the examination of the reactions to a given content: the more people react to it – comments, positive or negative rating, number of likes and so on – the more valuable the content seems to the machine algorithm which controlling the users' news feed. This means content that gets a lot of reactions will most likely be seen by many other users. Using a suitable, large enough botnet, the botmaster can increase the reach of targeted content – post, photo or video – when the botnet members react to it in sufficient numbers. Of course, the owners of social media platforms are also familiar with these practices and try to fight against them. One of the most serious social media competitors of traditional media is the platform called Twitter – many journalists and other reliable experts also publish on Twitter. Many people get information from there, though one of the main problems with Twitter is that it has a lot of "bots" that actively try to influence the reach of certain content. [3] In 2022, Elon Musk acquired Twitter – and since renamed it "X" – and softened the user validating methods. [4]

Another big issue of social media is the advertising model. The pivotal point of online advertising is the effectiveness of ads, and it can be significantly increased by appropriate targeting. Suppose someone is interested in a particular topic, such as searching for a washing machine on various websites. In that case, they are likely to respond more to a relevant ad than if it were only shown to random users. Because of the increased effectiveness, these properly targeted ads can be sold more expensively to advertisers. On the other hand, increased targeting requires data from user activities, interests and behavior which could be problematic from a data privacy point of view. Some platforms – like Facebook and Google Analytics – provide free services to third parties, but in return, they track the activities of their users and collect data from their online presence. [5]

Interest-based content positioning can be extremely dangerous for society. Public opinion could be manipulated efficiently if it is used to deliver a political message instead of advertising a commercial product or service. Social platforms usually have a direct connection interface – the API or Application Programming Interface – for larger business partners, usually advertisers. The main purpose of these interfaces is to provide useful targeting information to the partners, making them more profitable. Using this, the partner can select the group important to the advertiser businesses and display targeted content. One of the biggest such scandals erupted in 2018 after a whistleblower revealed that the British company Cambridge Analytica harvested data from 50 million Facebook users, and this data was used for profiling these users. [6] These profiles were used to influence the 2016 Trump campaign and probably the Brexit referendum. Using data mining procedures, they could produce lists from the retrieved data and target ads for these users based on their political views. Although the ethics of the procedure is questionable, according to the investigation, no violation of the law was committed, and the available tools were used. [7]

1.1.6 Spreading and Validating Propaganda

The World Wide Web contains much information and facts, and the total opposite claims can also be found. For the average reader, it is almost impossible to distinguish between the news and fake information, and sometimes alternative narratives are available for the same event. As the geopolitical situation in the world deteriorated, many armies started using psyops (Psychological Operations) to interfere with public opinion in "non-friendly" countries. Many propaganda organizations put publications on questionable authenticity and smaller websites, but their reach is very low and their effectiveness extremely poor. However, with a sufficiently large botnet and the involvement of the "influencer" users, it is possible to share and promote the content on social media, resulting in a drastic increase in the number of readers. As mentioned before, a broad readership also means more shares and likes, which means the content can reach many more readers indirectly. In addition, due to this indirect sharing mechanism, the credibility of the post will increase as more and more users share or use the false information. When the information from the untrustworthy original source reaches the appropriate level of credibility, the originator organization interested in spreading the propaganda begin to refer to it in different information channels.

The effect of spreading propaganda on public social media channels can be extremely dangerous. Between 2016 and 2017, the Myanmar military took advantage of the popularity of Facebook to conduct a targeted campaign against the local Muslim Rohingya minority, which resulted in genocide [8].

1.2 Internet of Things (IoT) Problems

As microelectronics develop, more computing power can fit smaller, cheaper devices. More computing power allows communication between these devices using computer networks, forming the so-called Internet of Things. The rise of IoT devices seems unstoppable. According to estimate, the number of "smart" devices connected to the Internet reached 14.3 billion at the end of 2022 and will reach 16.6 billion within a year.

These devices have relatively limited capacity, and their operating systems are very different. Many of them may contain security holes. If such a device is vulnerable, the entire network is at risk. As a result of, a successful attack, an IoT device can be a target, but it can also be a tool in DDoS or other attacks.

1.2.1 Mirai Botnet

The Mirai botnet consists of smart devices infected with malware running on ARC (Argonaut RISC Core) processors. These infected machines can be brought under central control and, therefore, can coordinate actions. In September 2016, the authors of the malware launched a DDoS attack against the website of a well-known security expert, and a week later, they made the source code public. Opening the source code of malware can provide a way to modify the original code more easily, and detecting these modifications will be much more difficult.

A serious mistake allowed the Mirai to infect devices automatically. Most manufacturers use the same stripped-down Linux operating system for the ARC processor, which had a default username-password pair for the root (administrator in Linux) user. If the password has yet to be changed by the manufacturer or the owner, Mirai malware could log in remotely and infect the system.

Infected devices can be baby monitors, vehicles, network switches, agricultural machinery, medical devices, meteorological devices, household appliances, video recorders, cameras, practically anything.

After the initial attack, the Mirai botnet disabled DynDNS using approximately 100,000 infected IoT devices. [10]

Because of the open-source code, the Mirai botnet has been mutated. The most recent version of Mirai can infect Android-based set-top-boxes and perform DDoS attacks with various methods. [11]

1.2.2 MQTT Attack

MQ Telemetry Transport (MQTT) is an application layer protocol used by remote monitoring and other data collection systems. Since 2016, it has become the reference standard for communication in Internet of Things (IoT) environments. Since more and more people are using it, its operational continuity is becoming more and more important. The protocol uses a publish/subscribe model; the central element is a server (broker), and clients can subscribe to it and will receive data automatically when it is available. The protocol was prepared to handle unreliable network connections. If the channel is broken, the broker stores the messages.

The Slow DoS against Internet of Things Environments (SlowITe) attack is based on the fact that the broker, prepared for slow, unreliable connections, is sufficiently “patient” with clients and does not disconnect from clients even when they are slow. The problem is exacerbated by the fact that MQTT uses TCP (Transmission Control Protocol) for communication.

The attacker initiates the connection with the CONNECT package, and the broker is obliged to maintain the connection for at least 60 seconds by default. To handle these connections, the server must use some resources. Too many connections could cause critical overuse of these resources. Therefore, the number of connections is limited. By creating the necessary number of connections, the attacker can prevent the creation of new connections while communicating with the broker as slowly as possible, thus prolonging the busy state as long as possible.

2 Artificial Intelligence and Botnets

In the last few years, Artificial Intelligence has been developed significantly, and Generative AI can generate – even photorealistic – images, videos and human-like texts. Generative AI is a collective term of different machine learning models and algorithms that can create new works similar to, but somehow different from the input data – basically man-made content – on which they were trained.

Using Long Language Models, the generated text content is surprisingly similar to human-made works; therefore, AI applications can drastically improve the efficiency of normal botnet activities. The following chapters will describe some new opportunities for this new technique.

2.1 Comment or Review Generation

Comments and reviews became important factors in public opinion about specific products or services. The so-called "review bombing" – when a large number of users leave negative comments – method can cause significant damage to any system where users are allowed to leave comments or reviews too easily. This phenomenon forced multiple websites to harden the review algorithms. [12] Generative AIs, with the help of LLMs, can generate human-like text very fast. A botnet operator could use this superb text-generation capability to create fake reviews, comments or other engagement posts to avoid the protective methods and algorithms.

2.1.1 Automated Social Engineering Attacks

LLMs can generate context-aware, highly convincing text. This capability allows the attacker to craft highly targeted, "spear-phishing" email or other social engineering attacks. A botnet could use LLMs to create personalized messages in large volumes that are more likely to trick users into clicking on dangerous links or other malicious content. Most spam and malware filter applications use simple statistical analysis or pattern-based lookup filtering to detect malicious content. Therefore, personalized messages can deceive the defense system.

Another method could be an LLM-capable chatbot. It can interact with the victims on different platforms – like social media or instant messaging systems – and behave like a human peer to extract sensitive information, spread propaganda or deliver malicious software payloads.

2.1.2 Advanced Phishing Attacks

An LLM-assisted botnet can create and deliver highly sophisticated phishing campaigns. It can generate convincing emails or other messages and deliver them to a forged – seemingly trusted – sender, making it difficult for users to distinguish between genuine and fake messages. Phishing attacks are very popular today, but most of the time, the phishing message is not convincing enough. Many of them contain spelling errors and poor wordings caused by poor translation. With the help of AI, these phishing emails can contain personal information of the victim, increasing the probability of a successful attack.

2.1.3 Disinformation and Manipulation

LLMs can generate fake news articles or social media posts. Botnets could employ AI to create large amounts of false information, contributing to more complex disinformation campaigns. Also, the false information can be amplified by a botnet large enough.

2.1.4 Personalized Scam

Nowadays, many scammers try to deceive innocent victims by spam emails with a special method called “Nigerian scam” or “419 scam”. This scam is based on the gullibility of people, it tries to convince the victim that large inheritance is available, but other transactions must be made before receiving it. These transactions usually involve money transferred to the scammer's bank account. Most of these scams are pretty dumb because all targets receive the same letter, and the content does not fit everyone. But if the attacker uses LLM, every target can receive a personalized letter with fitting data.

2.1.5 Fake Images and Videos

An Artificial Intelligence system can be trained on images and, with the help of advanced algorithms, can generate photorealistic or artistic images. Multiple systems are available today: Midjourney, Leonardo.AI. By generating convincing images and amplifying by a botnet, disinformation can spread quickly. With the current rate of development, separating fake and real pictures could be impossible, which can cause profound problems in society.

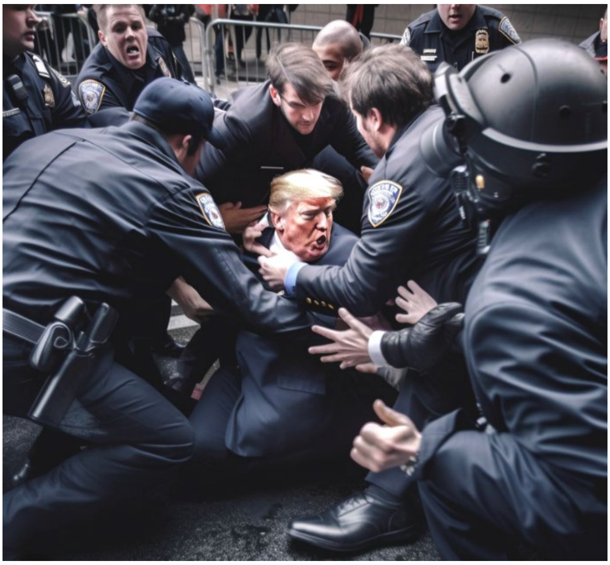


Figure 5
Fake picture generated by Midjourney. Source: Christo Gozev Twitter

Conclusions

The dangers posed by botnets are significant today, and the threat will be increasing in the future. In addition to the “traditional” areas of use – DDoS attacks sending spam – new attempts to influence the functioning of society are becoming more and more significant.

The spread of artificial intelligence is also a separate source of danger: Phishing emails will become less and less recognizable as different language models, such as GPT3 and GPT4, can produce convincing, personalized messages almost instantly. Besides the text content, image-generating systems can produce more and more believable fakes, so fake news is also becoming more and more believable. New problems have also emerged. Many AI systems are trained on data fetched from internet without the permission of the original author, and the copyright issues also work on the opposite side: who is the copyright owner of the generated content?

With the broadly used artificial intelligence applications, more and more content that contains nothing new based on previously existing information will be created. Finding factual, accurate information or honest opinions will become more and more complex, and the AI-generated “noise” will overshadow them.

These problems will generate significant social changes for which everyone should be prepared.

Acknowledgement

Óbuda University, Kandó Kálmán Faculty of Electrical Engineering supported this work.

References

[1] Omer Yoachimik, Julien Desgats, Alex Forster: Cloudflare mitigates record-breaking 71 million request-per-second DDoS attack [Online] Available: https://blog.cloudflare.com/cloudflare-mitigates-record-breaking-71-million-request-per-second-ddos-attack/

[2] Clipminer Botnet Makes Operators at Least $1.7 Million Symantec [Online] Available: https://symantec-enterprise-blogs.security.com/ blogs/threat -intelligence/clipminer-bitcoin-mining-hijacking

[3] Christoph Besel, Juan Echeverria, Shi Zhou: Full Cycle Analysis of a Large-scale Botnet Attack on Twitter [Online] Available: https://discovery.ucl.ac.uk/id/eprint/10074237/1/BotnetSpammingAttack_plain%20format.pdf

[4] Brian Fung: How Elon Musk transformed Twitter's blue check from status symbol into a badge of shame [Online] Available: https://edition.cnn.com/2023/04/24/tech/musk-twitter-blue-check-mark/index.html

[5] David Brokaw: Facebook's "Like" Button Plugin and User Tracking: Stretching Outdated and Ambiguous Laws to Protect User Privacy, 17 J. Bus. & Tech. L. 89 (2022) [Online] Available: https://digitalcommons.law.umaryland.edu/jbtl/vol17/iss1/5

[6] Carole Cadwalladr and Emma Graham-Harrison: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach [Online] Available: https://www.theguardian.com/news/2018/mar/17/ cambridge-analytica-facebook-influence-us-election

[7] BBC News: Cambridge Analytica 'not involved' in Brexit referendum, says watchdog [Online] Available: https://www.bbc.com/news/uk-politics-54457407

[8] Paul Mozur, The New York Times: A Genocide Incited on Facebook, With Posts from Myanmar's Military [Online] Available: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

[9] Satyajit Sinha: State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally [Online] Available: https://iot-analytics.com/number-connected-iot-devices/

[10] CloudFlare: What is the Mirai Botnet? [Online] Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[11] Bill Toulas: Mirai variant infects low-cost Android TV boxes for DDoS attacks [Online] Available: https://www.bleepingcomputer.com/news/security/mirai-variant-infects-low-cost-android-tv-boxes-for-ddos-attacks/

[12] Christine Fischer: Metacritic changes its user review policy to combat score bombing [Online] Available: https://www.engadget.com/metacritic-score-bombing-game-review-changes-150200740.html