Бояринова Анна Геннадьевна
студентка
Научный руководитель
Савина Светлана Владимировна
канд. физ.-мат. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

CYBERATTACKS OF COMPANIES IN SOCIAL MEDIA AND HOW TO PROTECT AGAINST THEM

Аннотация*: в статье рассмотрено влияние кибератак на социальные меди, обозначены способы защиты от них. Автором проанализированы методы и мотивы кибератак, описаны их типы. Статья содержит всю необходимую для компаний информацию о кибератаках и киберугрозах.*

Ключевые слова*: кибератаки, социальные медиа, хакеры, киберугрозы, защита от кибератак.*

Abstract*: in this article, the impact of cyberattacks on social media and ways of their prevention are considered. Methods and motives of cyberattacks are analyzed, and the types of cyberattacks are described. The article contains all the information a company needs to know about cyberthreats and cyberattacks.*

Keywords*: cyberattacks, social media, hackers, cyberthreats, protection against cyberattacks.*

Social media isn't just about promoting your brand, picking the coolest hashtags, or getting political arguments that come to nothing. Social media is also a cyber risk for your company. Social networks have become a platform for cybercriminals. At least one in eight major corporations will have security breaches due to hackers on social media in the coming new year. Cyberattacks are an unauthorized exposure to a com-

puter system with special software in order to disrupt its operation, obtain secret information. Social platform attacks target websites with large user bases, such as Facebook, LinkedIn, Twitter, and Instagram. A majority of current attacks simply use the social platforms as a delivery mechanism, and have been modeled after the older Koobface malware. However, researchers are now anticipating that advanced attacks against social media networks will be able to leverage a user's contacts, location, and even business activities. This information can then be used to develop targeted advertising campaigns toward specific users, or even help spark crime in the virtual or real world. Most often, attacks on social media platforms can compromise user accounts, stealing their authentication credentials when logging in to the system. This information is then used to covertly extract personal data from users ' online friends and colleagues. A recent Stratecast study claims that 22% of social media users were victims of a security-related incident, and recent documented attacks support these figures. The pony botnet has affected Facebook, Google, Yahoo and other social media users, stealing more than 2 million user passwords. Facebook estimates that anywhere from 50 million to 100 million of its monthly active user accounts are fake duplicates, and as many as 14 million of them are «unwanted» on the site.

Anything you post online these days is fair game to crooks. Your organization needs to know the best ways to protect itself. In an era of file sharing on steroids, you must face this reality head on. Organizations should embrace security-aware culture. Make sure each and everyone of your employees understands the potential risks involved in using social media on work desktops, laptops, or mobile devices. There are easy steps that employees can take. The most obvious one being, limiting what outsiders are able to find out about them. In this current world of showing off online, a CEO might be better off having employees who shy away from the social media spotlight. They need to refuse friend requests from people they don't know and never click on suspicious links.

Cyberattacks take advantage of vulnerabilities, whether it's weaknesses in software, computing devices, or the humans that administer and use them. As websites

grow more complex and applications are developed more rapidly, the potential for attack increases. Meanwhile, hackers and cyber-mercenaries are building, distributing, and utilizing sophisticated exploit tools and malware to steal or destroy critical corporate data, compromise Web sites, and disrupt operational infrastructures.

Whether the motive is espionage or sabotage, cyber criminals employ a range of attack methods, such as spear-phishing, SQL injection attack, cross-site scripting (XSS), and brute force attacks, using them adaptively and in combination to carry out elaborate cyberattacks.

One of the most disruptive tactics used in cyberattacks is the distributed denial of service (DDoS) attack in which botnets are used to congest a website or web application to the point that legitimate users can no longer access it-costing enterprises millions of dollars in revenue, lost productivity and damaged reputations.

Government organizations and financial firms remain the focus of many cyberattacks, particularly those carried out in the name of hacktivism. However, due to the open infrastructure of the Internet and the increased availability of easy-to-implement attack tools, almost anyone with the basic skills necessary can carry out a cyberattack, making cyber security a top priority for any enterprise with valuable digital assets and an Internet presence. Social networks have been growing immensely in the amount of data it receives from its users. It is noteworthy to mention laws in different countries that have been taken place in order to guide the companies holding this user information accountable should there be any data breach. Given the efforts placed around by the various infrastructures, this paper is not geared towards understanding what those laws or set standards are, instead we are geared towards understanding what the social network and social media profile data mean to an attacker.

There are many types of cyberattacks:

– Distributed Denial-of-service (DDoS) attack: a malicious attempt to slow down or crash a website by flooding it with overwhelming amounts of traffic. Cybercriminals achieve this by using large armies of automated «bots» and create large-scale attacks;

– malware: a malicious code designed to cause damage to a computer or network. There is a wide range of different malware categories, including but not limited to worms, trojans, spyware, and keyloggers;

– phishing: the act of attempting to trick the recipient of a malicious email into opening and engaging with it. The «sender» of the email deceives the victim by making the email appear to be sent from a reputable source, such as a government department, a supplier, or a customer of the business;

– SQL injection: these attacks take advantage of vulnerabilities in the database layer of an application. Hackers inject malicious SQL queries into a website entry field, tricking the application into executing unintended commands, and penetrate the backend database;

– man-in-the-middle attack: mostly happening on unsecured pubic Wi-Fi, these attacks consist in the hackers interrupting the traffic between a visitor device and a network, insert themselves into a two-party transaction to steal data without the visitor's knowing;

– brute force attack: also referred to as password cracking, brute force attacks are typically carried out to discover log-in credentials and gain access to websites for the purposes of data theft, vandalism, or the distribution of malware, which in turn can be used to launch brute force, DDoS and various types of cyberattacks on other targets. Even without successfully penetrating an online property, brute force attacks can flood servers with traffic, resulting in significant performance issues for the site under attack;

– breach attack: these attacks compromise the privacy goal of SSL by reducing HTTPS to encrypting page headers, leaving other content susceptible to discovery. Using a combination of brute force attacks and divide-and-conquer techniques, these attacks can be employed by hackers to extract login credentials, email addresses, and other sensitive, personally identifiable information from SSL-enabled websites.

Organizations, particular those that have suffered the effects of cyberattacks, have strengthened perimeter-based security controls like firewalls and intrusion detection systems. Unfortunately, traditional data center security methods such as these are not

enough to protect companies from large-scale, distributed cyber threats and furtive attacks at the application layer. What enterprises need today are multi-layered defense architectures that can not only detect and deflect cyberattacks as close to the source as possible but also scale to absorb massive-scale threats.

Список литературы

1. Sood A. Targeted cyberattacks: multi-staged attacks driven by exploits and malware / A. Sood, R. Enbody. – Elsevier Science, 2014. – 158 p.

2. Cyberattacks [Электронный ресурс]. – Режим доступа: www.akamai.com/us/en/resources/cyber-attacks.jsp

3. Social cyberattacks and how to protect against them [Электронный ресурс]. – Режим доступа: https://mondo.com/blog-social-cyberattacks

4. Social Media Cyber Attack Risks [Электронный ресурс]. – Режим доступа: https://nordic-backup.com/blog/social-media-cyber-attack-risks/