DOI: 10.34185/1991-7848.itmm.2020.01.043

АНАЛІЗ СУЧАСНОГО СТАНУ СПАМ-ТРАФІКУ В КОНТЕКСТІ ПИТАНЬ КІБЕРБЕЗПЕКИ

Гнатушенко В.В., д.т.н., Блат О.Л., студентка групи КН901-14-М

НМетАУ, Україна

Ключові слова: ПОШТОВИЙ ТРАФІК, СПАМ, СТАТИСТИЧНИЙ ЛІНГВІСТИЧНИЙ АНАЛІЗ, ФІШИНГ, КІБЕРБЕЗПЕКА, КІБЕРНЕБЕЗПЕКА.

Вступ. Нині роль електронних засобів передачі даних у сучасному суспільстві дедалі підвищується. Всебічна діджиталізація та електронна комерція торкаються усіх видів людської діяльності. У цих умовах підвищується роль електронної пошти як одного з найважливіших засобів мережних комунікацій. На жаль, в останні роки у світі намітилася негативна тенденція щодо застосування комунікаційних ресурсів електронної пошти в спам-бізнесі. Масштаби спам-розсилок набувають таких розмірів, які загрожують безпеці Інтернету в цілому, тому задача боротьби з цим негативним явищем сьогодні, як ніколи, актуальна.

Ця робота присвячена проблемам всебічного аналізу сучасного стану світових спам-процесів, нових інформаційних технологій масових поштових розсилок та оцінці кіберзагроз, що супроводжують такі процеси.

Основний матеріал. За даними інтелектуальної платформи аналізу кіберзагроз Cisco Talos [1], частка спаму у загальному світовому поштовому трафіку у 2019 році становила близько 85%. Також проаналізовано загальний розподіл спаму за країнами світу [2]: основними джерелами спаму є Китай (20% від світового обсягу) та США (14%); частка спаму з України складає близько 2%.

Слід зазначити, що сьогодні спам являє собою не просто шкідливий трафік, який призводить до втрат робочого часу, коштів та перевантажує канали передачі даних. Спам, насамперед, це – серйозна загроза безпеці систем зберігання та обробки даних. Технології спам-розсилок сприяють розповсюдженню мережних вірусів, malware-загроз, а спам-фішинг створює умови для масового Інтернет-шахрайства. Так, річний звіт з кібербезпеки Cisco [3] наводить приклади випадків, що сталися у 2017 році. Серед них –

масштабна атака, спрямована на персональні дані користувачів Gmail [4], злам енергетичних систем Ірландії, розповсюдження програми-здирника Jaff великою бот-мережею Necurs [5] тощо.

Авторами був проведений власний статистичний аналіз розподілу спаму на базі поштової системи mail.lanservice.net, яка обслуговує кілька досить великих корпоративних користувачів. Сервери цієї системи розташовані у найкрупнішому датацентрі міста Варшави (Польща). Поштова система обслуговує 12 поштових доменів, деякі з яких функціонують більш ніж 20 років. Поштовий трафік був проаналізований на підставі лог-файлів зазначеної поштової системи, де збиралася детальна статистика загальних запитів до системи за різними протоколами, статистика запитів, які були відхилені та кваліфіковані як спам тощо. Таку статистику було проаналізовано за період з 2016 по 2020 роки з деталізацією за годину, добу, тиждень, місяць, рік. Отримані результати добре корелюють з наведеними вище показниками.

Таким чином, визначення ключових джерел спам-трафіку та активний пошук шляхів його мінімізації є дуже актуальною задачею з точки зору ефективності роботи інформаційних систем та їх кібербезпеки.

Враховуючи, що, спам-листи не мають формальних особливих ознак та часто маскуються під звичайну чесну кореспонденцію, ефективні методи боротьби із сучасним спамом мають базуватися, насамперед, на статистичному лінгвістичному аналізі вмісту поштових відправлень. У той самий час, це – окрема проблема, яка виходить за рамки нашої роботи та буде розглянута у подальшому.

Висновки. На підставі авторитетних аналітичних джерел та за власними даними проведено детальні дослідження і аналіз сучасного спаму та джерел його розповсюдження. Показано, що сучасний спам являє собою елемент кібернебезпеки, яку необхідно ефективно усувати. Намічені шляхи подальших досліджень у цьому напрямку, які, насамперед, пов’язані з розробкою ефективних технологій протидії спаму, які базуються на статистичному лінгвістичному аналізі вмісту поштових відправлень.

Література

1. Email & Spam Data. Total Global Email & Spam Volume for January 2020 // Cisco Talos. URL: https://talosintelligence.com/reputation_center/email_rep (дата звернення: 10.02.2020).
2. Мария Вергелис, Татьяна Сидорина, Татьяна Щербакова. Спам и фишинг в третьем квартале 2019 года // Лаборатория Касперского. URL: https://securelist.ru/spam-report-q3-2019/95097/ (дата звернення: 10.02.2020).
3. Річний звіт Cisco з кібербезпеки за 2018 рік // Cisco Systems, Inc. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html (дата звернення: 10.02.2020).
4. Alex Johnson. 12 Massive Phishing Attack Targets Gmail Users // NBC News. URL: https://nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-754501 (дата звернення: 10.02.2020).
5. Nick Biasini, Edmund Brumaghin, Warren Mercer. Jaff Ransomware: Player 2 Has Entered the Game // Блог Cisco Talos. URL: blog.talosintelligence.com/2017/05/jaff-ransomware.html (дата звернення: 10.02.2020).

THE SPAM TRAFFIC ACTUAL STATE ANALYSIS IN THE CONTEXT OF CYBERSECURITY ISSUES

Gnatushenko Viktorija, Blat Olha

Annotation. The detailed analysis of the actual situation with Internet spam traffic is given. Spam traffic is investigated by various aspects: by countries, by topics, by types of the dangers that accompany the corresponding spam mailings etc. The thesis about spam risks increasing and the necessity for effectively deal with it is proposed as a result of the shown researches. Modern spam technologies are quite various and flexible, they often based on methods of social engineering using. Therefore the ways to deal with such threats should also be non-trivial.

Keywords: MAIL TRAFFIC, SPAM, STATISTICAL LINGUISTIC ANALYSIS, PHISHING, CYBER SECURITY, FISHING, CYBER THREAT.

References

1. Email & Spam Data. Total Global Email & Spam Volume for January 2020 // Cisco Talos. URL: https://talosintelligence.com/reputation_center/email_rep (the date of application: 10.02.2020).

2. Maryia Verhelys, Tatiana Sydoryna, Tatiana Shcherbakova. Spam y fyshynh v tretem kvartale 2019 hoda // Laboratoryia Kasperskoho. URL: https://securelist.ru/spam-report-q3-2019/95097/ (the date of application: 10.02.2020).

3. Richnyi zvit Cisco z kiberbezpeky za 2018 rik // Cisco Systems, Inc. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html (the date of application: 10.02.2020).

4. Alex Johnson. 12 Massive Phishing Attack Targets Gmail Users // NBC News. URL: https://nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-754501 (the date of application: 10.02.2020).

5. Nick Biasini, Edmund Brumaghin, Warren Mercer. Jaff Ransomware: Player 2 Has Entered the Game // Блог Cisco Talos. URL: blog.talosintelligence.com/2017/05/jaff-ransomware.html (the date of application: 10.02.2020).