


Chapter 25

The Anatomy of Phishing Attacks and the Detection and Prevention of Fake Domain Names

Erkan Şen

Nebula Bilişim Sistemleri Sanayi ve Ticaret Ltd. Şti., Turkey

Gurkan Tuna

 <https://orcid.org/0000-0002-6466-4696>

Trakya University, Turkey

ABSTRACT

Internet technology and its infrastructure are getting more and more into our lives. In parallel with this, there is an increase in the number of phishing attacks that rely on fake/deceptive domain names. Web-based phishing attacks aim at obtaining users' (individual/corporate) personal and/or financial information by using fake domain names. Within the scope of this chapter, firstly, phishing attacks are explained. How they are prepared and implemented is examined. Then, the steps to be taken to detect fake domain names to which users are directed are examined.

INTRODUCTION

With the emergence of internet technologies in all areas of life, the number of attacks has begun to increase rapidly. Identity theft has emerged as a type of attack with many financial, military and commercial goals. Web phishing attacks, on the other hand, have become one of the most used methods for identity theft. Phishing attacks carry out these attacks by convincing that the web application they are in is real and they can cause great harm to both the relevant users and the targeted institutions such as the loss of reputation and money (Kalaycı, 2021).

DOI: 10.4018/978-1-6684-3380-5.ch025

Table 1. Web phishing statistics Q1 2021

Number of	January	February	March
Number of unique phishing sites detected	245,771	158,898	207,208
Number of unique phishing email headers	172,793	112,369	39,918
Number of brands targeted by phishing campaigns	430	407	465

As the internet usage and internet fraud headlines reflected in the news increase, users' interest in this subject also increases. For this reason, attackers are using more sophisticated and convincing methods for phishing attacks every day. According to the Anti-Phishing Attack Working Group (APWG) 2021 Q1 report, the number of unique phishing sites detected on the Internet has reached 611,877 in total. Table 1 reveals the magnitude of the threat (Anti Phishing Work Group, 2021).

In phishing attacks, attacks are prepared using different methods, depending on the target population/institution and the desired result. Although the used methods vary, the main point where the attackers build the attack is the domain name. Web phishing attacks are widely used today to deceive end users and seize their information. Therefore, it is imperative for institutions to take measures against these attacks. For individuals, the high probability of success of these attacks and the scarcity of measures should also be taken into account. With on-site detection and notification, end-users' exposure to these attacks can be minimized.

In phishing attacks, while transitioning from the planning stage to the application/campaign stage, fake domain name registrations are made, similar to the real domain name, according to the target institution/population. It is important that these records are identified quickly and consistently around the world. Findings need to be delivered to institutions and end users as quickly as possible and ready for use. In this regard, the purpose of this research is to analyze the phishing attacks carried out using fake/imitation domain names and to provide the necessary technical information to detect the relevant domain names that form the cornerstone of these attacks in order to prevent them. This research does not cover all the methods of phishing attacks and focuses on the correct and accurate detection of domain names used in phishing attacks using a novel algorithm. However, due to the nature of the Internet, like defense methods, attack methods are also developing and evolving.

IDENTITY THEFT AND WEB PHISHING ATTACKS

Identity theft is a malicious behavior that has existed since ancient times. With the widespread use of information systems, we have new identities in almost every medium. This can sometimes refer directly to our official identity as well as social media, online gaming etc. It can also belong to a virtual personality that does not actually exist on platforms. These identities carry characters that have both material and spiritual reflections. Identity theft is generally defined as the unauthorized use of information describing an individual/institution, in whole or in part, by another without the consent of him or a legal authority (Newman, 2005). Modern identity thieves try to obtain all kinds of information that represents us in the digital environment. Such information may include but not be limited to:

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/the-anatomy-of-phishing-attacks-and-the-detection-and-prevention-of-fake-domain-names/299203

Related Content

Towards Public Services and Process Integration: A Domain-Specific Modeling Approach

Guillermo Infante Hernández, Aquilino A. Juan Fuente, Benjamín López Pérez and Edward Rolando Núñez-Valdéz (2015). *Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications* (pp. 2100-2112).

www.irma-international.org/chapter/towards-public-services-and-process-integration/127955

Government Spending Transparency on the Internet: An Assessment of Greek Bottom-Up Initiatives over the Diavgeia Project

Evika Karamagioli, Eleni-Revekka Staiou and Dimitris Gouscos (2014). *International Journal of Public Administration in the Digital Age* (pp. 39-55).

www.irma-international.org/article/government-spending-transparency-on-the-internet/106543

On-Site Clinics: A New Model of Health Coverage in Local Government

Robert Yehl, Mary Eleanor Wickersham and Virginia B. Sizemore (2016). *Social, Economic, and Political Perspectives on Public Health Policy-Making* (pp. 213-232).

www.irma-international.org/chapter/on-site-clinics/145894

Defense Acquisition, Public Administration, and Pragmatism

Keith F. Snider (2017). *Emerging Strategies in Defense Acquisitions and Military Procurement* (pp. 186-204).

www.irma-international.org/chapter/defense-acquisition-public-administration-and-pragmatism/160519

Inter-organizational Transactions Cost Management with Public Key Registers: Findings from the Netherlands

Walter T. de Vries and Hanneke Ester (2015). *International Journal of Public Administration in the Digital Age* (pp. 22-32).

www.irma-international.org/article/inter-organizational-transactions-cost-management-with-public-key-registers/121534