Chapter 35
Spear Phishing:
The Tip of the Spear Used by Cyber Terrorists

Arun Vishwanath
University at Buffalo, USA

ABSTRACT

The ubiquitous use of the Internet has made it possible for terrorist groups to remotely foment attacks with little risk of capture. Among the newest forms of attacks is cyber hacking, which has seen increased use by terrorist groups for acts ranging from pinpointing targets for assassination to holding organisations hostage and embarrassing governments. In almost all these attacks, spear phishing is the vector used to gain access to a computer network – making it imperative that policymakers find ways to stop it. This chapter provides an overview of the different types of spear phishing attacks and the reasons they succeed. The chapter then provides an overview of the different strategies being used to combat it and their relative effectiveness. Drawing from the latest social science research and from initiatives that have worked around the world, the chapter culminates with six policy suggestions, which could significantly reduce the effectiveness of spear phishing and protect nations from a major cyber attack.

INTRODUCTION

Terrorism is broadly defined as the unlawful use of force or violence to intimidate or coerce a civilian population or government to further political or social objectives (Federal Bureau of Investigation [FBI], n.d.). In the not so distant past, such acts required terrorists to physically enter national boundaries and conduct acts of terror. Geography, border security, and the risk of capture often limited the scope of these attacks. Our dependence on the Internet for all manner of activities, from the household monitoring of thermostats to the control of a nation's electric grid, and its democratised nature – the lack of gatekeepers (such as the editors of traditional news), the availability of standardised operating platforms, and open source software – have made it easier for today's terrorist groups to remotely foment acts of terror without the risk of capture.

DOI: 10.4018/978-1-5225-7909-0.ch035

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Ongoing news reports of Al-Qaeda and the Islamic State in Iraq and Syria (ISIS) using YouTube, Twitter, and Facebook to disseminate videos of successful attacks, recruit individuals, and promote propaganda demonstrate how technically adept these groups have become (Hingham & Nakashima, 2015). But there is another troubling trend: the use of spear phishing attacks by terrorist groups.

In December 2014, ISIS launched a spear phishing attack on citizen media groups sympathetic to the Syrian government – an attack intended to place position-beacons in individual computers that could reveal the sympathisers' locations, presumably for assassination (Scott-Railton & Hardy, 2014). In another attack, ISIS used spear phishing to gain access to the U.S. Military Central Command's (Centcom) Twitter and YouTube accounts, and on the very day that U.S. President Obama made a speech on cyber security, posted images with threats against American soldiers (Zetter, 2015).

ISIS, however, is not alone. Another prolific hacker group, the Syrian Electronic Army (SEA), with links to Syria, Iran, and Hezbollah, recently hacked the Twitter account of the Associated Press (AP) and tweeted false news to AP's 2-million plus followers of two explosions in the White House that injured U.S. President Obama. Although the hack was quickly discovered and a correction sent out within three minutes of the tweet, by then the Dow Jones had dropped 143-points (Shell, 2013), and the S&P (Standard and Poor's) Index had lost USD 136 billion (Prigg, 2015). SEA has also defaced websites of news media they considered hostile to the Syrian government such as BBC News and The New York Times; defaced Facebook pages of President Obama and French President Nicholas Sarkozy; and also hacked into the recruiting websites of the U.S. Marine Corps (Acohido, 2013). Other reports of Palestinian hackers using spear phishing attacks to breach computer networks of the Israeli Defense Force (IDF) (Fisher-Ilan & Finkle, 2014); of the Iranian sponsored hacker group Tahr Andishan breaching Saudi Aramco, the state-owned national oil company of Saudi Arabia, in retaliation for Saudi Arabia government's support for sanctions against Iran (Nakashima, 2012); and of Russian hackers breaching German Chancellor Angela Merkel's computers ("Russian hackers accused", 2015), demonstrate the variety of groups utilising such modus operandi.

Almost all these major breaches have one thing in common: they all extensively utilise spear phishing. Figure 1 presents the lifecycle of a breach. As shown in the figure, spear phishing is usually the first step in a typical hacking attack that leads to a breach. It is often used early for initial information gathering, for locating individuals, and for gauging the interest of potential targets. This is usually accomplished by assessing target individuals' reactions to emails sent with varying information cues (headers, subject-line, reply-to address, etc.) or by getting access to individuals' social media accounts using fake friend requests. This data-mined information is often used to craft more targeted malware-carrying spear phishing emails, which then allow the phisher to establish a foothold, maintain presence, move laterally to other computers or vertically to other connected servers and escalate access, and finally accomplish the breach. Thus, spear phishing is the proverbial 'tip of the spear' used by cyber terrorists all over the world to launch hacking attacks with goals ranging from cyber espionage and terrorism to vandalism and acts intended to embarrass individuals, governments, and organisations – making it the focus of this chapter.

On incidence terms, the U.S Defense Department receives upwards of ten million attacks per day; many states in the United States receive twice as much; organisations, especially those in telecommunications, technology, banking and insurance industries, also receive just as many (Vishwanath, 2015a). On monetary terms, cyber breaches have shown the potential to net rich dividends. Compared to the estimated USD 120 million that Al-Qaeda netted over an eight-year period from ransoms (Callimachi, 201), a hacker group from Ukraine recently netted in excess of USD 100 million over a five-year period by spear phishing and hacking into several financial news organisations, and selling advance trade in-

14 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/spear-phishing/220967

Related Content

The Influence of the Cultural and Linguistic Orientations of Sultan Qaboos University (SQU) Students on Their Responses to Literatures on the Internet
Rahma Al-Mahrooqiand Victoria Tuzlukova (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 687-699).*
www.irma-international.org/chapter/influence-cultural-linguistic-orientations-sultan/42812

Preventing Cyberbullying and Online Harassment
Jess Nerren (2022). *Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 1419-1443).*
www.irma-international.org/chapter/preventing-cyberbullying-and-online-harassment/301699

The Impact of Mindfulness Practices and the Implementation of Technology in Higher Education
Shaakira Sharif, Aubrey Stattiand Kelly M. Torres (2022). *Impact and Role of Digital Technologies in Adolescent Lives (pp. 124-145).*
www.irma-international.org/chapter/the-impact-of-mindfulness-practices-and-the-implementation-of-technology-in-higher-education/291362

The Net Generation and E-Textbooks
Arlene J. Nicholasand John K. Lewis (2011). *International Journal of Cyber Ethics in Education (pp. 70-77).*
www.irma-international.org/article/net-generation-textbooks/56110

Smart Phone Security Practices: Item Analysis of Mobile Security Behaviors of College Students
Scott E. Menschand LeAnn Wilkie (2019). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-14).*
www.irma-international.org/article/smart-phone-security-practices/236157